# Principles of Registry Ethics, Data Ownership, and Privacy

Draft Chapter for Third Edition of "Registries for Evaluating Patient Outcomes: A User's Guide"

## 1. Introduction

This chapter covers the ethical and legal considerations that should accompany the development and use of all health information registries, including patient registries as defined in this document, for the purposes of public health activities, governmental health program oversight, quality improvement/assurance (I/A), and research. These considerations apply generally accepted ethical principles for scientific research involving human subjects to health information registries. Related topics include issues of transparency in the operation of registries, oversight of registry activities, and property rights in health care information and registries.

Section 2.1 of this chapter discusses the ethical concerns and considerations involved with obtaining and using confidential health information in registries. Section 2.2 describes the transformation of ethical concerns into the legal regulation of human subjects research and individually identifiable health information. In Section 3, an overview is presented of these regulatory requirements and their interactions as they specifically relate to registries. Section 4 makes recommendations about registry transparency and oversight, based on the need to ensure the independence, integrity, and credibility of biomedical research, while preserving and improving the utility of registry data. Finally, property rights in health information and registries are briefly discussed. Table , at the end of this chapter, provides an overview of the applicable regulatory requirements based on the type of registry developer and the extent to which registry data are identifiable.

The purpose of this chapter is solely to provide information that will help readers understand the issues, not to provide specific legal opinions or regulatory advice. Legal advisors should always be consulted to address specific issues and to ensure that all applicable Federal, State, and local laws and regulations are followed. The discussion below about legal protections for the privacy of health information focuses solely on U.S. law. Health information is also legally protected in European and some other regions by distinctly different rules, none of which are discussed in this chapter.[1] If registry developers intend to obtain health information from outside of the United States or transfer to or share their information with registries outside the United States, they should consult legal counsel early in the registry planning

process for the necessary assistance. It should also be noted that the rules and regulations described here are for the protection of patients and research participants, not to prevent legitimate research. While the requirements may seem daunting, they are not insurmountable barriers to research. With careful planning and legal guidance, registries can of course be designed and operated in compliance with applicable rules and regulations.

In the context of this chapter, *health information* is broadly construed to include any individual patient information created or used by health care providers and insurance plans that relates to a health condition, the provision of health care services, or payment for health care services.[2] As a result, health information may include demographic information and personal characteristics, such as socioeconomic and marital status, the extent of formal education, developmental disability, cognitive capacities, emotional stability, as well as gender, age, and race, all of which may affect health status or health risks. Health information, as defined here, should be regarded as intimately connected to individual identity, and thus, intrinsically private. Typically, health information includes information about family members, so it also can have an impact on the privacy of third parties. Patients widely regard health information as a confidential communication to a health care provider and expect confidentiality to be maintained.

Serious concerns about potential risks to individual privacy have led to Federal legal requirements for prospective review of registry projects and specific permissions to use health information for research purposes. The creation and use of patient registries for a research purpose ordinarily constitute "research involving human subjects" as defined by regulations applicable to research activities funded by the U.S. Department of Health and Human Services[3] (HHS) and certain other Federal agencies. Moreover, Federal privacy regulations resulting from the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[4] the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Reinvestment and Recovery Act of 2009,[5] and the rules promulgated thereunder specifically apply to the use and disclosure of certain individually identifiable health information for research and other purposes.

The term *human subjects* is used throughout this chapter for consistency with applicable Federal law. Some may prefer the term *research participants*.

This chapter provides a general guide to Federal legal requirements in the United States. (Legal requirements in other countries may also be relevant and may be different from those in this country, but even a general discussion of applicable international rules is beyond the scope of this document.) These legal requirements may influence registry decisions involving the selection of data elements and data verification procedures, and may also affect subsequent uses of registry data for secondary research

purposes. State laws also may apply to the use of health information for research purposes. The purpose of a registry, the status of its developer, and the extent to which registry data are identifiable largely determine applicable regulatory requirements. This chapter reviews the most common of these arrangements. The complexity and sophistication of registry structures and operations vary widely, with considerable variability also observed in the processes used by registry stewards to obtain data. Nonetheless, common ethical and legal principles are associated with the creation and use of registries. These commonalities are the focus of this chapter.

Ethical concerns about the conduct of biomedical research, especially research involving the interaction of the clinical research community with their patients and commercial funding agencies, have produced an impetus to make financial and other arrangements more public. The discussion of transparency in this chapter includes recommendations for the public disclosure of registry operations as a means of maintaining public trust and confidence in the use of health information. Reliance on a standing advisory committee is recommended to registry developers as a way to provide expert technical guidance for registry operations and to firmly establish the independence of the registry from committed or conflicted interests, as described in Chapter 2. This discussion of transparency in methods is not intended to discourage private investments in registries that produce proprietary information in some circumstances. Neither the funding source nor the generation of proprietary information from a registry determines whether a registry exercises and adheres to the good practices described in this guide.

Registry developers are likely to encounter licensing requirements, including processing and use fees, in obtaining health and claims information. Health care providers and health insurance plans have plausible claims of ownership to health and claims information, although the public perspective on these claims has not been tested. Registry developers should anticipate negotiating access to health and claims information, especially when it is maintained in electronic form. The processes for use of registry datasets, especially in multiple analyses by different investigators, should be publicly disclosed if the confidentiality protections required for health information are to remain credible.

# 2. Ethical Concerns Relating to Health Information Registries

## *2.1. Application of Ethical Principles*

The Belmont Report[6] is a summary of the basic principles and guidelines developed to assist in resolving ethical problems in the conduct of research with human subjects. It was the work product of the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, which was created by the National Research Act of 1974.[7]

The Belmont Report identifies three fundamental principles for the ethical conduct of scientific research that involves human subjects. These principles are respect for persons as autonomous agents (self-determination), beneficence (do good; do no harm; protect from harm), and justice (fairness; equitable distribution of benefits and burdens; equal treatment). Together, they provide a foundation for the ethical analysis of human subjects research, including the use of health information in registries developed for scientific purposes with a prospect of producing social benefits. These principles are substantively the same as those identified by the Council for International Organizations of Medical Sciences (CIOMS) in its international guidelines for the ethical review of epidemiologic studies.[8]

Nevertheless, the application of these principles to specific research activities can result in different conclusions about what comprises ethical design and conduct of the research in question. These different conclusions frequently occur because the principles are assigned different values and relative importance when more than one person performs the ethical analysis. In most of these situations, however, a generally supported consensus position on the ethical design and conduct of the research is a desired and achievable goal. This goal does not preclude re-analysis as social norms or concerns about research activities change over time in response to new information, new technologies or persistent ethical questioning.

The ethical principle of *respect for persons* supports the practice of obtaining individuals' consent to the use of their health information for research purposes that are related or unrelated to the clinical and insurance reasons for creating the information. In connection with research registries, consent may have multiple components: (1) consent to registry creation by the compilation of patient information; (2) consent to the initial research purpose and uses of registry data; and (3) consent to subsequent use of registry data by the registry developer or others for the same or different research purposes. The consent process should adequately describe registry purposes and operations to inform potential subjects' decisions about participation in a research registry. In some defined circumstances, the principle of *respect for persons* may be subordinate to other ethical principles and values, with the result that an explicit consent process for participation in the registry may not be necessary. A waiver of informed consent requirements may apply to the registry and be ethically acceptable. (See discussion of waivers of informed consent requirements in Section 3.3.5.) In these situations, alternatives to an explicit consent process for each individual contributing health information to the registry may be adequate. For example, the registry might provide readily accessible, publicly available information about its activities as an alternative to individual informed consent.

A general ethical requirement for consent clearly implies that human subjects voluntarily permit the use of their health information in a registry, unless a specific exception to voluntary participation applies to the registry. One such exception is a legally mandated, public health justification for the compilation of health information (e.g., certain infectious disease reporting). Voluntary agreement to the use of health information in a registry necessarily allows a subsequent decision to discontinue participation. Any limitation on an individual's ability to withdraw information from the registry (e.g., once incorporation into aggregated data has occurred) should be clearly communicated in the consent process as a condition of initial participation. The consent process should also include instructions about the procedures for withdrawal at any time from participation in the registry unless a waiver of consent applies to the registry. Incentives for registry use of health information (e.g., insurance coverage of payments for health care services) should be carefully evaluated for undue influence both on the individuals whose health information is sought for registry projects and on the health care providers of those services.[9,10]

Conflicts of interest may also result in undue influence on patients and may compromise voluntary participation. One potential source of conflict widely identified within clinical research is the use of recruitment incentives paid by funding agencies to health care providers.[11] Some professional societies and research organizations have established policy on the use of recruitment incentives. Many entities have characterized as unethical incentives that are significantly beyond fair market value for the work performed by the health care provider; others require disclosure to research subjects of any conflicting interest, financial or nonfinancial.[12] There is now Federal legislation that requires manufacturers of certain drugs, devices, or medical supplies to report, for public display, the amounts of remuneration paid to physicians for research purposes.[13] Some States, including Massachusetts, have similar laws in effect.[14] Research organizations, particularly grantees of Federal research funding, may have systematic policies and procedures in place that registry developers can rely on for managing employee conflicts of interest. Nonetheless, in their planning, registry developers should specify and implement recruitment practices that protect patients against inappropriate influences.

Applying the principle of *respect for persons* to the research use of health information generates additional ethical concerns about preserving the privacy and dignity of patients, protecting the confidentiality of health information, and minimizing potential harms. These concerns have intensified as health care services, third-party payment systems, and health information systems have become more complex. Legal standards for the use and disclosure of health information have replaced professional and cultural norms for handling individually identifiable health information. Nonetheless, depending on the particular health condition or population of interest, safeguards for the confidentiality of registry data

beyond applicable legal requirements may be ethically necessary to protect the privacy and dignity of those individuals contributing health information to the registry.

The principle of *beneficence* ethically obligates developers of health information registries for research purposes to minimize potential harms to the individuals or groups[15] whose health information is included in the registry. There are usually no apparent benefits to offset potential harm to the individuals or groups whose health information is used in the registry. Exceptions to this arise when a registry is designed to provide benefits to the human subjects as individuals, such as longitudinal reports on treatment effects or health status or quality-of-care reports. Risks to privacy and dignity are minimized by conscientious protection of the confidentiality of the health information included in the registry[16] through the use of appropriate physical, technical, and administrative safeguards for data in the operations of the registry. These safeguards should also include controls on access to registry data, including access to individual identifiers that may be included in registry data. Minimization of risks also requires a precise determination of what information is necessary for the research purposes of the registry.

Certain populations of patients may be vulnerable to social, economic, or psychological harms as a result of a stigmatizing health condition. Developers of registries compiling this health information must make special efforts to protect the identities of the human subjects contributing data to the registry. Additional legal protections may apply if HHS-supported research is being conducted through or in connection with the registry. Additional protections also apply to populations such as pregnant women, human fetuses, neonates, prisoners, and children, who are considered vulnerable to undue influence and coercion during the consent process. In particular, data obtained from pediatric and adolescent populations may lead to ethical concerns if there is the potential for lifelong discrimination that may effectively exclude them from educational opportunities and other social benefits[17] (e.g., health care insurance, although under the Affordable Care Act health insurers may not discriminate against individuals on the basis of pre-existing conditions).

In an analysis applying the principle of *beneficence*, research involving human subjects that is unlikely to produce valid scientific information is unethical. This conclusion is based on the lack of social benefit to offset even minimal risks imposed by the research on participating individuals. Health information registries should incorporate an appropriate design (including, where appropriate, calculation of the patient sample as described in Chapter 3) and data elements, written operating procedures, and documented methodologies, as necessary, to ensure the fulfillment of a valid scientific purpose.[18]

An ethical analysis employing the principle of *justice* also yields candid recognition of the potential risks to those who contribute health information to a registry, and the probable lack of benefit to those

individuals (except in the cases where registries are specifically constructed to provide benefit to those individuals). The imbalance of burden and benefit to individuals emphasizes the need to minimize the risks from registry use of health information. Precise and well-developed scientific reasons for inclusion (or exclusion) of defined health information in a registry help ensure that the burden placed on individuals as a result of their participation is fair and equitable.

The above analysis refers to research activities. However, the ethical concerns expressed may also apply to other activities that use the health information of individuals in scientific endeavors solely for non-research purposes. Public health, oversight of the delivery of health care services through government programs, and quality I/A activities all can evoke the same set of ethical concerns as research activities about the protection of patient self-determination, privacy, and dignity; the maintenance of the confidentiality of individually identifiable health information to avoid potential harms; and the imposition of a risk of harm on some individuals to the benefit of others not at risk. In the past, different assignments of social value to these activities and different potential for the social benefits and harms they produce have created different levels of social acceptance and formal oversight for these activities compared with research activities. Nonetheless, these activities may include a research component in addition to their stated objectives, a circumstance that reinforces the ethical concerns discussed above and produces additional concerns about compliance with the legal requirements for research activities. Registry developers should prospectively apply careful scrutiny to the proposed purposes for and activities of a registry, in consultation with appropriate institutional officials, to avoid both ethical and compliance issues that may undermine achievement of the registry's objectives.

Registry developers must also consider confidentiality and/or proprietary concerns with regard to the identity of the health care providers, at the level of both individual professionals and institutions, and the health care insurance plans from which they obtain registry data. Information about health care providers and insurance plans can also identify certain patient populations and, in rare circumstances, individual patients. Moreover, the objectives of any registry, broadly speaking, are to enhance the value of the health care services received, not to undermine the credibility and thus the effectiveness of health care providers and insurance plans in their communities. Developers of registries created for public health investigations, health system oversight activities, and quality I/A initiatives to monitor compliance with recognized clinical standards must consider whether safeguards for the identity of service professionals and institutions are appropriate. At the same time, however, any confidentiality safeguards should permit certain disclosures, as designated by the service professionals and institutions, for the reporting of performance data, which are increasingly associated with payment from payers.

## 2.2. Transformation of Ethical Concerns Into Legal Requirements

Important ethical concerns about the creation, maintenance, and use of patient registries for research purposes include risks of harm to human subjects resulting from unauthorized access to registry data and inappropriate use of the compiled health information. These concerns about harms arise from public expectations of confidentiality for health information and the importance of that confidentiality in preserving the privacy and dignity of individual patients as well as the clincian/patient relationship.

Over the last decade, two rapid technological developments have intensified these ethical concerns. One of these advances was DNA sequencing, replication, recombination, and the concomitant application of this technology to biomedical research activities in human genetics. Widespread anticipation of potential social benefits produced by biomedical research as a result of these technologies was accompanied by ethical concern about the potential for affronts to personal dignity and economic, social, or psychological harms to individuals or related third parties.

In addition to specific ethical concerns about the effect of technological advances in biomedical research, general social concerns about the privacy of patient information have accompanied the advance of health information systems technology and electronic information processing, as applied to the management and communication of health information. These social concerns produced legal protections, first in Europe and later in the United States. The discussion below about legal protections for the privacy of health information focuses solely on U.S. law.

### 2.2.1. The Common Rule

International and domestic concerns about the protection, respect, and privacy of human subjects resulted in a uniform set of regulations from the Federal agencies that fund such research known as the "Common Rule."[19,20] The legal requirements of the Common Rule apply to research involving human subjects conducted or supported by the 17 Federal departments and agencies that adopted the Rule. Some of these agencies may require additional legal protections for human subjects. The HHS regulations will be used for all following references to the Common Rule.

Among these requirements is a formal written agreement, from each institution engaged in such research, to comply with the Common Rule. For human subjects research conducted or supported by most of the Federal entities that apply the Common Rule, the required agreement is called a Federalwide Assurance (FWA).[21] Research institutions may opt in their FWA to apply Common Rule requirements to all human subjects research activities conducted within their facilities or by their employees and agents, regardless of the source of funding. The application of Common Rule requirements to a particular registry depends

on the institutional context of the registry developer, relevant institutional policies, and whether the health information contributed to the registry maintains patient identifiers.

The Office for Human Research Protections (OHRP) administers the regulation of human subjects research conducted or supported by HHS. Guidance published by OHRP discusses research use of identifiable private health information. This guidance makes clear that OHRP considers the creation of health information registries for research purposes containing individually identifiable, private information to be human subjects research for the institutions subject to its jurisdiction.[22] The applicability of the Common Rule to research registries is discussed in more detail in Section 4.

OHRP regulations for human subjects protection require prospective review and approval of the research by an institutional review board (IRB) and the informed consent (usually written) of each of the human subjects involved in the research, unless an IRB expressly grants a waiver of informed consent requirements.[23] A research project must satisfy certain regulatory conditions to obtain IRB approval of a waiver of the informed consent requirements. (See Section 3.3.5. for discussion of waivers of informed consent requirements.) A registry plan is the research "protocol" reviewed by the IRB. At a minimum, the protocol should identify (1) the research purpose of a health information registry, (2) detailed arrangements for obtaining informed consent, or detailed justifications for not obtaining informed consent, to collect health information, and (3) appropriate safeguards for protecting the confidentiality of registry data, in addition to any other information required by the IRB on the risks and benefits of the research.[24]

As noted previously, for human subjects research conducted or supported by most Federal departments and agencies that have adopted the Common Rule, an FWA satisfies the requirement for an approved assurance of compliance. Some research organizations extend the application of their FWA to all research, regardless of the funding source. Under these circumstances, any patient information registry created and maintained within the organization may be subject to the Common Rule. In addition, some research organizations have explicit institutional policies and procedures that require IRB review and approval of all human subjects research.

### 2.2.2. The Privacy Rule

In the United States, HIPAA and the HITECH Act, enacted as part of the American Reinvestment and Recovery Act of 2009, and their implementing regulations[25] (here collectively called the Privacy Rule) created legal protections for the privacy of individually identifiable health information created and maintained by so-called "covered entities" and their "business associates." "Individually identifiable health information" is information, including demographic data, that relates to an individual's 1) past,

present, or future physical or mental health condition; 2) health care provisions; or 3) past, present, or future payment for health care provisions. The Privacy Rule refers to this information as "protected health information" (PHI). Because registries may exist over long periods of time, it is important to note that the Privacy Rule does not protect individually identifiable information of persons who have been deceased for more than 50 years.

Covered entities are health care providers that engage in certain financial and administrative health care transactions electronically, health plans, and health care clearinghouses.[26] Business associates are persons or organizations, other than a member of a covered entity's workforce, that perform certain functions or services (e.g., claims processing, data analysis, data aggregation, patient safety activities) on the covered entity's behalf involving the use or disclosure of individually identifiable health information.[27] For the purposes of this chapter, the relevant entities are covered health care providers, which may include individual health care providers (e.g., a physician, pharmacist, or physical therapist), health care insurance plans, and their business associates. The discussion in this chapter assumes that the data sources for registries are covered entities or their business associates to which the Privacy Rule applies. In the unlikely event that a registry developer intends to collect and use data from sources that are not covered entities or their business associates under the Privacy Rule, such as personal health record vendors that are not working on behalf of a covered entity or business associate, these sources are subject only to applicable State law and accreditation requirements, if any, for patient information.

Although data sources are assumed to be subject to the Privacy Rule, registry developers and the associated institutions where the registry will reside may not be. Notably, the Privacy Rule does not apply to registries that reside outside of a covered entity, unless: 1) a registry is working on behalf of a covered entity to perform a covered function or service, or 2) a registry is otherwise providing data transmission services involving protected information to a covered entity. These functions or services require routine access by the registry to the protected health information. These cases, in which the registry would be considered a business associate, trigger applicability of certain provisions of the HIPAA Privacy Rule and the HIPAA Security Rule. Within academic medical centers, for example, registry developers may be associated with units that are outside of the institutional health care component to which the Privacy Rule applies, such as a biostatistics or economics department. But because many, if not virtually all, data sources for registries are covered entities or their business associates, registry developers are likely to find themselves deeply enmeshed in the Privacy Rule. This involvement may occur with noncovered entities as well—for instance, as a result of business practices developed in response to the Privacy Rule. In addition, the formal agreements required by the Privacy Rule in certain circumstances in order to access, process, manage, and use certain forms of patient information impose legally enforceable continuing

conditions upon users of data under contract law. Such conditions of use may result in direct liability under HIPAA if the registry is considered a business associate of a data source that is a covered entity. Therefore, registry developers should become cognizant of the patient privacy considerations confronting their likely data sources as well as themselves if they are performing functions or services on behalf of their data sources (business associate) and should consider following certain Privacy Rule procedures, required or not, depending on their arrangements with those data sources.

In general, the Privacy Rule defines the circumstances under which health care providers and insurance plans (covered entities) and their business associates may use and disclose patient information for a variety of purposes, including research. Existing State laws protecting the confidentiality of health information that are contrary to the Privacy Rule are preempted, unless the State law is more protective (which it may be).[28] For example, the Privacy Rule requires that certain information be present in patient authorizations to use and disclose individually identifiable information, including an expiration date. The laws of the State of Maryland, however, specifically require that, absent certain exceptions, a patient's authorization may only be valid for a maximum period of one year.[29] As a result, a covered entity located in Maryland must comply with the State's one-year maximum expiration deadline on its patient authorization forms.

The Privacy Rule regulates the use of identifiable patient information within health care providers' organizations and insurance plans, and the disclosure of patient information to others outside of the institution (e.g., their business associates) that create and maintain the information.[30] The initial collection of registry data from covered entities or business associates is subject to specific Privacy Rule procedures, depending on the registry's purpose, whether the registry resides within a covered entity or outside of a covered entity, whether the registry is considered a business associate of the covered entity, and the extent to which the patient information identifies individuals. Health care providers or insurance plans, as well as their business associates, that create, use, and disclose patient information for clinical use or business purposes are subject to civil and criminal liability for violations of the Privacy Rule.

Registry developers should be sufficiently knowledgeable about the Privacy Rule to facilitate the necessary processes for their data sources or their business associates. In developing a registry, they should expect to interact with clinicians, the Privacy Officer, the IRB or Privacy Board staff, health information system representatives, legal counsel, compliance officials, and contracting personnel. Registry developers should also maintain awareness of modifications, amendments, or new implementing regulations under the Privacy Rule, which can be expected as the use of electronic health information becomes more prevalent. For example, on January 25, 2013, HHS issued significant modifications to the

Privacy Rule required by the HITECH Act.[31] One of the most relevant modifications for registry developers and health information exchanges is the extension of Privacy Rule requirements and enforcement directly to business associates, including health information organizations engaged in electronic data transmission.[32]

Subsequent use and sharing of registry data may be affected by the regulatory conditions that apply to initial collection, as well as by new ethical concerns and legal issues. The Privacy Rule created multiple pathways by which registries can compile and use patient information. To use or share compiled registry data for research purposes, a registry developer may need to employ several of these pathways sequentially and satisfy the regulatory requirements of each pathway. For instance, a registry within a covered entity may arrange to obtain written documentation of an authorization required by the Privacy Rule from each patient contributing identifiable information to a registry for a particular research project, such as the relationship between hypertension and Alzheimer's disease. If the registry subsequently seeks to use the data for another research purpose, it may do so if it obtains another permission in the Privacy Rule—for example, by obtaining additional patient authorizations or first de-identifying the data to Privacy Rule standards.

The authors recommend that registry developers establish a detailed tracking system, based on the extent to which registry data remain identifiable for individual patients, for the collection, uses, and disclosures of registry data. The tracking system should produce comprehensive documentation of compliance with both Privacy Rule requirements and legally binding contractual obligations to data sources.

With regard to registries developed for research purposes, the Privacy Rule defines research as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."[33] Commentary by HHS on the Privacy Rule explicitly includes within this definition of research the development (building and maintenance) of a repository or database for future research purposes.[34] The definition of research in the Privacy Rule partially restates the definition of research in the preexisting Common Rule for the protection of human subjects enacted by the HHS and other Federal agencies.[35] Some implications of this partial restatement of the definition of research are discussed later in this chapter.

The National Institutes of Health (NIH) has published guidance on the impact of the Privacy Rule on health services research and research databases and repositories. The NIH guidance identifies the options available to investigators under the Privacy Rule to gain access to health information held by health care providers and insurance plans.[36] In addition to provisions for the use or disclosure of identifiable patient information for research, the Privacy Rule permits health care providers and insurance plans and their

business associates to use or disclose patient information for certain defined public health activities.[37] The Privacy Rule defines a public health authority as "an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency… that is responsible for public health matters as part of its official mandate."[38] The Centers for Disease Control and Prevention (CDC) and HHS have jointly published specific guidance on the Privacy Rule for public health activities.[39] Other Privacy Rule provisions permit the use or disclosure of patient health information as required by other laws.[40]

The protections for patient information created by the Privacy Rule that are generally relevant to registries developed for research purposes include explicit individual patient authorization for the use or disclosure of identifiable information,[41] legally binding agreements for the release of "limited datasets" between health information sources and users,[42] the removal of specified identifiers or statistical certification to achieve de-identification of health information,[43] an accounting of disclosures to be made available to patients at their request,[44] and notification in the event of a breach of unsecured protected health information to affected individuals who may be harmed by the breach. In addition, if certain criteria required by the Privacy Rule are satisfied, an IRB or Privacy Board may grant a waiver of individual patient authorization for the use or disclosure of health information in research.[45]

### 2.2.3. FDA Regulations

U.S. Food and Drug Administration (FDA) regulatory requirements for research supporting an application for FDA approval of a product also include protections for human subjects, including specific criteria for protection of privacy and maintaining the confidentiality of research data.[46]

### 2.2.4. Applicability of Regulations to Research; Multiple-Purpose Registries

At many institutions, the IRB or the office that provides administrative support for the IRB is the final arbitrator of the activities that constitute human subjects research, and thus may itself determine what activities require IRB review. A registry developer is strongly encouraged to consult his or her organization's IRB or a central IRB as applicable early in the registry planning process to avoid delays and lessen the need for multiple revisions of documentation submitted to the IRB. Distinctions between research and other activities that apply scientific methodologies are frequently unclear. Such other activities include both public health practice[47] and quality-related investigations.[48] Both the ostensible primary and secondary purposes of an activity are factors considered in the determination of whether registry activities constitute research subject to the Common Rule. As interpreted by OHRP, if any secondary purpose of an activity is research, then the activity should be considered research.[49] This

OHRP interpretation of research purpose differs from that of the Privacy Rule with respect to quality-related studies performed by health care providers and insurance plans. Under the Privacy Rule, only if the primary purpose of a quality-related activity is to obtain generalizable knowledge do the research provisions of the Privacy Rule apply; otherwise, the Privacy Rule defines the activity as a "health care operation."[50]

Registry developers should rely on their Privacy Officer's and IRB's experience and resources in defining research and other activities for their institutions and determining which activities require IRB review as research. In response to accreditation standards, inpatient facilities typically maintain standing departmental (e.g., pediatrics) or service (e.g., pharmacy or nursing) committees to direct, review, and analyze quality-related activities. Some physician groups also establish and maintain quality-related programs, because good clinical practice includes ongoing evaluation of any substantive changes to the standard of care. These institutional quality committees can provide guidance on the activities that usually fall within their purview. Similarly, public health agencies typically maintain systematic review processes for identifying the activities that fit within their legal authority.

As mentioned previously, use of registry data for multiple research purposes may entail obtaining additional permissions from patients or satisfying different regulatory requirements for each research purpose. Standard confidentiality protections for registry data include requirements for physical, technical, and administrative safeguards to be incorporated into plans for a registry. In some instances, an IRB may not consider legally required protections for the research use of patient information sufficient to address relevant ethical concerns, including the protections of the Privacy Rule that may be applicable to registries created and maintained within health care providers and insurance plans as covered entities or business associates. For example, information about certain conditions (such as alcoholism or HIV-positive status) and certain populations (such as children) may be associated with a greater potential for harm from social stigma and discrimination. Under these circumstances, the IRB can make approval of a registry plan contingent on implementation of additional safeguards that it determines are necessary to minimize the risks to the individuals contributing health information to the registry.

## 3. Applicable Regulations

This section discusses the specific applicability of the Common Rule[51] and the Privacy Rule[52] to the creation and use of health information registries. Registry developers are strongly encouraged to consult with their organization's Privacy Officer and IRB or Privacy Board early in the planning process to

clarify applicable regulatory requirements and the probable effect of those requirements on registry design and development.

This discussion assumes three general models for health information registries. One model is the creation of a registry containing the contact, demographic, and diagnostic or exposure information of potential research subjects who will be individually notified about projects in which they may be eligible to participate. The notification process permits the registry to shield registry participants from an inordinate number of invitations to participate in research projects, as well as to protect privacy and confidentiality. This model is particularly applicable to patients with unusual conditions, patients who constitute a vulnerable population,[53] or both (e.g., children with a rare condition). A second model is the creation of a registry and the conduct of all subsequent research using registry data by the same group of investigators. No disclosures of registry data will occur and all research activities have the same scientific purpose. This model applies, in general, to quality improvement registries and other quality-related investigations of a clinical procedure or service. Note, however, that some quality improvement registries may involve confidential feedback to providers as well as public reporting of provider performance in a patient de-identified format. These activities may or may not constitute research as defined by HIPAA and the Common Rule, but instead may be regulated as the health care operations of the covered entity that provides the data to the registry. A third model is the creation of a registry for an initial, specific purpose by a group of investigators with the express intent to use registry data themselves, as well as to disclose registry data to other investigators for additional related or unrelated scientific purposes. An example of this last model is a registry of health information from patients diagnosed with a condition that has multiple known comorbidities to which registry data can be applied. This third model is most directly applicable to industry-sponsored registries. The American College of Epidemiology encourages the data sharing contemplated in this last registry model.[54] Data sharing enhances the scientific utility of registry data and diminishes the costs of compilation.

The extent to which the regulations will apply to each of these registry models will depend on factors such as the registry developer, purpose of the registry, potential for individual patient identification, consent process, and inclusion of genetic information. These factors are discussed further below.

## 3.1. Public Health, Health Oversight, FDA-Regulated Products

When Federal, State, or municipal public health agencies create registries in the course of public health practice, specific legislation typically authorizes the creation of the registries and regulates data acquisition, maintenance, security, use, and disclosures of registry data for research. Ethical considerations and concerns about maintaining the confidentiality of patient information used by public

health authorities are similar to those for research use, but they are explicitly balanced against potential social benefits during the legislative process. Nonetheless, if the registry supports human subjects research activities as well as its public health purposes, Common Rule requirements for IRB review may apply to the creation and maintenance of the registry.

Cancer registries performing public health surveillance activities mandated by State law are well-known exceptions to Common Rule regulation. However, secondary uses of public health registry data for research and the creation of registries funded by public health agencies, such as the CDC and the Agency for Healthcare Research and Quality (AHRQ), may be subject to the Common Rule as sponsored research activities. The Common Rule's definitions of human subjects research[55] may encompass these activities, which are discussed in the next subsections of this chapter. Not all cancer registries support public health practice alone, even though the registries are the result of governmental programs. For example, the Surveillance Epidemiology and End Results (SEER) program, funded by the National Cancer Institute, operates and maintains a population-based cancer reporting system of multiple registries, including public use datasets with public domain software. SEER program data are used for many research purposes in addition to aiding public health practices. These latter research activities may be subject to the Common Rule. [56]

Disclosures of health information by health care providers and insurance plans and their business associates for certain defined public health activities are expressly recognized as an exception to Privacy Rule requirements for patient authorization.[57] An example of a public health activity is the practice of surveillance, in which the distributions and trends of designated risk factors, injuries, or diseases in populations are monitored and disseminated.[58] Health care providers or insurance plans are likely to demand documentation of public health authority for legal review before making any disclosures of health information. Registry developers should obtain this documentation from the agency that funds or enters into a contract for the registry, and present it to the health care provider or insurance plan well in advance of data collection efforts.

The Privacy Rule permits uses and disclosures by health care providers and insurance plans and their business associates for "health oversight activities" authorized by law.[59] These activities include audits and investigations involving the "health care system" and other entities subject to government regulatory programs for which health information is relevant to determining compliance with program standards.[60] The collection of patient information, such as occurrences of decubitus ulceration, from nursing homes that are operating under a compliance or corporate integrity agreement with a Federal or State health care program, is an example of a health oversight activity.

The Privacy Rule characterizes responsibilities related to the quality, safety, or effectiveness of a product or activity regulated by FDA as public health activities. This public health exception for uses and disclosures of patient information in connection with FDA-regulated products or activities includes adverse event reporting; product tracking; product recalls, repairs, replacement, or look-back; and postmarketing surveillance (e.g., as part of a risk management program that is a condition for approval of an FDA-regulated product).[61]

## 3.2. Research Purpose of a Registry

The Common Rule defines research, and its definition is partially restated in the Privacy Rule, as described earlier. These regulatory definitions affect how the regulatory requirements of each rule are applied to research activities.[62]

In the Common Rule:

> Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. Activities which meet this definition constitute research for purposes of this policy, whether or not they are conducted or supported under a program which is considered research for other purposes. For example, some demonstration and service programs may include research activities.[63]

OHRP interprets this Common Rule definition of research to include activities having *any* research purpose, no matter what the stated objectives of the activity may be. Compliance with Common Rule requirements depends on the nature of the organization where the registry resides. If an organization receives Federal funding for research, then it is likely that Common Rule requirements apply.

The Privacy Rule's definition of research[64] restates the first sentence of the Common Rule definition. However, the Privacy Rule distinguishes between research and quality I/A or patient safety activities conducted by covered entities or their business associates,[65] which are defined as "health care operations."[66] As a result, if the primary purpose of a quality or patient safety-related registry maintained by a covered entity is to support a research activity (i.e., to create generalizable knowledge), Privacy Rule requirements for research apply to the use or disclosure of the patient information to create the registry and to subsequent research use of registry data. If, however, the primary purpose is other than to create generalizable knowledge, the study is considered a health care operation of the covered entity and is not subject to Privacy Rule requirements for research activities or patient authorization.

As noted earlier, both public health practice and quality I/A or patient safety activities can be difficult to distinguish from research activities.[67] The determination of whether a particular registry should be

considered as or include a research activity depends on a number of different factors, including the nature of the organization where the registry will reside; the employment duties of the individuals performing the activities associated with the registry; the source of funding for the registry; the original, intended purpose of the registry; the sources of registry data; whether subsequent uses or disclosures of registry data are likely; and other circumstances of registry development.

Quality I/A activities entail many of the same ethical concerns about protecting the confidentiality of health information as research activities do. Express consent to quality I/A activities is not the usual practice; instead, the professional and cultural norms of health care providers, both individual and institutional, regulate these activities. Registry developers should consider whether the ethical concerns associated with a proposed quality I/A or patient safety registry require independent review and the use of special procedures such as notice to patients or providers. Registry advisory committee members, quality I/A and patient safety literature,[68] hospital ethics committees, IRB members, and clinical ethicists can make valuable contributions to these decisions.

To avoid surprises and delays, the decision about the nature of the activity that the registry is intended to support should be made prospectively, in consultation with appropriate officials of the funding agency and officials of the organization where the registry will reside. Some research institutions may have policies that either require IRB review for quality I/A or patient safety activities, especially if publication of the activity is likely, or exclude them from IRB review. Frequently, IRBs make this determination on a case-by-case basis.

## 3.3. Potential for Individual Patient Identification

The specific regulatory requirements applicable to the use or disclosure of patient information for the creation of a registry to support human subjects research depend in part on the extent to which patient information received and maintained by the registry can be attributed to a particular person. Various categories of information, each with a variable potential for identifying individuals, are distinguished in the Privacy Rule: *individually identifiable* health information, *de-identified* information (all identifying elements removed), and a *limited dataset* of information (certain identifiers removed).[69] The latter two categories of information may or may not include a code linked to identifiers.

If applicable, Common Rule requirements affect all research involving patient information that is individually identifiable and obtained by the investigator conducting the research. The definition of "human subject" in the Common Rule is "a living individual about whom an investigator (whether professional or student) conducting research obtains (1) data through intervention or interaction with the individual, or (2) identifiable private information."

This regulatory definition further explains that:

> Private information includes…information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (for example, a medical record). Private information must be individually identifiable (i.e., the identity of the subject is or may readily be ascertained by the investigator or associated with the information) in order for obtaining the information to constitute research involving human subjects.[70]

In short, the Common Rule definition of *human subject* makes all research use of identifiable patient information subject to its requirements; if the identity of the patients whose information is used for research purposes is not readily ascertainable to the investigator, the research is not human subjects research to which the Common Rule applies. Moreover, research involving the collection of information from existing records is exempt from the Common Rule if the information is recorded by the investigator in such a manner that subjects cannot be identified, directly or through a coded link to identifiers. Registry developers should consult the IRB early in the process of selecting data elements to obtain guidance about whether registry activities constitute human subjects research or may be exempt from Common Rule requirements.

Also among the criteria specified by the Common Rule for IRB approval of research involving human subjects are provisions to protect the privacy of subjects and to maintain the confidentiality of data.[71] In addition, the consent process for research subjects should include explicit information about the confidentiality protections in place when records containing identifiers are going to be used.[72]

Data collection frequently requires patient identifiers, especially in prospective registries with ongoing data collection, revision, and updates. Secondary or subsequent research use by outside investigators (i.e., those not involved in the original data collection) of patient information containing direct identifiers is complicated, however, because ethical principles for the conduct of human subjects research require that risks, including risks to confidentiality of patient identifiable information, be minimized. In addition, the Privacy Rule requires patient authorization to specifically describe the purpose of the use or disclosure of patient information. Unless the registry developer has anticipated the purposes of secondary research, the initial authorization received from a patient may not constitute authorization for the use of identifiable registry data for secondary research purposes. The Privacy Rule provides options for the collection and use of identifiable health information to a greater or lesser extent, and also establishes standards for de-identifying information and for creating limited datasets.[73] Chapter 16 provides a discussion of the technical and legal considerations related to linking registry data for secondary research purposes.

Direct identifiers, as specified by the Privacy Rule, may include a patient's name, contact information, medical record number, and Social Security Number, alone or in combination with other information. As stated in the Privacy Rule standard, a limited dataset of patient information does not include specified direct identifiers of the patient, or the patient's relatives, employer, or household members.[74]

In an electronic environment, masking of individual identities is a complex task. Data suppression limits the utility of the information from the registry. Linkage or triangulation of information can re-identify individuals. A technical assessment of electronic records for their uniqueness within any dataset is necessary to minimize the potential for re-identification. In aggregated published data, standard practice assumes that a subgroup size of less than six may also be identifiable, depending on the nature of the data. An evaluation for uniqueness should be performed to ensure that the electronic format does not produce a potential for identification greater than this standard practice, including when the information is triangulated within a record or linked with other data files.

If a registry for research, public health, or other purposes will use any of the categories of health information discussed below, a registry developer should consult the IRB, the Privacy Officer, and the institutional policies developed specifically in response to the Privacy Rule early in his or her planning. These consultations should establish the purpose of the registry, the applicability of the Common Rule requirements to registry activities, and the applicability of the Privacy Rule to the collection and use of registry data. In addition, the registry developer should consult a representative of the information technology or health information system office of each health care provider or insurance plan that will be a source of data for the registry, as well as a representative of the IRB or Privacy Board for each data source, so as to obtain feasibility estimates of data availability and formats.

### 3.3.1. De-Identified Patient Information

The Privacy Rule describes two methods for de-identifying health information.[75] One method requires the removal of certain data elements. The other method requires a qualified statistician to certify that the potential for identifying an individual from the data elements is very small. A qualified statistician should have "appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable" in order to make this determination.[76] De-identified information may include a code permitting re-identification of the original record by the data source (covered entity).[77] The code may not be derived from information about an individual, including hash codes,[78] and should resist translation. In addition, the decoding key must remain solely with the health care provider or plan that is the source of the patient information.[79]

Research using existing data in which individual patients cannot be identified directly or indirectly through linked identifiers does not involve human subjects as defined by the Common Rule, and thus is not subject to the requirements of the Rule.[80] Refer to the discussion later in this chapter.

As a prudent business practice, each health care provider or insurance plan or their business associate that is a source of de-identified information is likely to require an enforceable legal agreement with the registry developer. It should be signed by an appropriate institutional official on behalf of the registry developer. At a minimum, this agreement will likely contain the following terms, some of which may be negotiable: the identification of the content of the data and the medium for the data; a requirement that the data recipient, and perhaps the health care provider or insurance plan or their business associate providing the data, make no attempt to identify individual patients; the setting of fees for data processing and data use; limitations on disclosure or further use of the data, if any; and an allocation of the risks of legal liability for any improper use of the data.

### 3.3.2. Limited Datasets of Health Information

De-identified health information may not suffice to carry out the purposes of a registry, especially if the registry is designed to receive followup information as a result of monitoring patients over time or information from multiple sources in order to compile information on a health event (e.g., cancer incidence). Dates of service and geographic location may be crucial to achieving the purposes of the registry or to the integrity and use of the data. Health information provided to the registry without direct identifiers may constitute a *limited dataset* as defined by the Privacy Rule.[81] A health care provider or insurance plan or their business associate (if permitted by the terms of the business associate arrangement) may disclose a limited dataset of health information by entering into a data use agreement (DUA) with the recipient. The terms of the DUA should satisfy specific Privacy Rule requirements.[82] Institutional officials for both the data source and the registry developer should sign the DUA so that a legal contract results. The DUA establishes the uses of the limited dataset permitted to the registry developer (i.e., the creation of the registry and subsequent use of registry data for specified research purposes). The DUA may not authorize the registry developer to use or disclose information in a way that would result in a violation of the Privacy Rule by either the data source or their business associate.[83] Furthermore, the DUA for a limited dataset of health information should require the data recipient to warrant that no attempt will be made to identify the health information with individual patients or to contact those patients.[84]

An investigator who works for a health care provider or insurance plan to which the Privacy Rule applies and that is the source of the health information for a registry may use a limited dataset to develop a

registry for a research purpose. In these circumstances, the Privacy Rule still requires a DUA that satisfies the requirements of the Privacy Rule between the health care provider or insurance plan and the investigator. This agreement may be in the form of a written confidentiality agreement.[85]

A registry developer may assist a health care provider or insurance plan or their business associate by creating the limited dataset.[86] In some situations, this assistance may be crucial to ensuring that data are accessible and available to the registry. In order for the registry developer to create a limited dataset on behalf of a data source, the Privacy Rule requires that the data source (the covered entity or their business associate) and the registry developer (in this instance acting as a business associate) enter into a business associate agreement that satisfies certain regulatory criteria.[87] The business associate agreement is a binding legal arrangement that should be signed by appropriate institutional officials on behalf of the data source and registry developer. This agreement should include terms for managing health information as required by the Privacy Rule.[88] Most health care providers have developed a standard business associate agreement in response to the Privacy Rule and will likely insist on using it, although some modifications may need to be negotiated in order to produce registry data.

The registry populated with a limited dataset may include a coded link that connects the data back to patient records. The key to the code (e.g., encryption key) may allow health information obtained from patients over time to supplement existing registry data or allow the combination of information from multiple sources.

If the registry data obtained by investigators constitute a limited data set, then the research does not involve human subjects, as defined by HHS regulations at 45 Code of Federal Regulations (CFR) 46.102(f), and the Common Rule requirements would not apply to the registry.[89] An IRB or an institutional official knowledgeable about the Common Rule requirements should make the determination of whether a research registry involves human subjects; frequently, a special form for this purpose is available from the IRB. The IRB (or institutional official) should provide the registry developer with documentation of its decision.

### 3.3.3. Direct Identifiers: Authorization and Consent

As discussed above, the Privacy Rule permits the use or disclosure of patient information for research with a valid, written authorization from each patient whose information is disclosed.[90] The Privacy Rule specifies the content of this authorization, which gives permission for a specified use or disclosure of the health information.[91] Health care providers and insurance plans frequently insist on using the specific authorization forms that they have developed in order to avoid legal review and minimize any potential liability that they believe might be associated with use of other forms.

One exception to the requirement for an authorization occurs when a health care provider or insurance plan creates a registry to support its "health care operations."[92] Health care operations specifically include quality I/A and patient safety activities, outcomes evaluation, and the development of clinical guidelines; however, the Privacy Rule definition of health care operations excludes research activities.[93] For example, a hospital registry created to track its patient outcomes against a recognized clinical care standard as a quality improvement initiative has a health care operations purpose. The hospital would not have to obtain an authorization from its patients for use of the health information it tracks in this registry.

Research use of health information containing identifiable information constitutes human subjects research as defined by the Common Rule.[94] In general, the Common Rule requires documented, legally effective, voluntary, and informed consent of each research subject.[95]

Documentation of the consent process required by the Common Rule may be combined with the authorization required by the Privacy Rule for disclosure and use of health information.[96] A health care provider or insurance plan may not immediately accept the combination of these forms as a valid authorization and may insist on legal review of the combination form before permitting disclosure of any health information.

Authorizations for the use or disclosure of health information under the Privacy Rule and informed consent to research participation under the Common Rule must be legally effective (i.e., obtained from a legally competent subject or the subject's legally authorized representative and documented in a manner consistent with the regulations and applicable laws of the jurisdiction). Adults, defined in most States as at least 18 years old, are generally presumed legally competent in the absence of a judicially approved guardianship. Minors are frequently defined as individuals under 18 years old and are presumed legally incompetent; therefore, a biological, adoptive, or custodial parent or guardian must provide permission on the child's behalf. Registry developers should consult legal counsel about situations in which these presumptions seem inapplicable, such as when a registry is created to investigate contraceptive drug and device use by adolescents, where State law exceptions may exist.

In addition to being voluntary and legally effective, an individual's consent should be informed about the research, including what activities are involved, as well as the expected risks and potential benefits from participation. The Common Rule requires the consent process to include specific elements of information.[97] Registry developers should provide non-English-speaking patients with appropriate resources to ensure that the communication of these elements during the consent process is comprehensible. All written information for patients should be translated, or else arrangements should be made for qualified translators to attend the consent process.

IRBs may approve waivers for both authorization (for disclosure of patient information for registry use) and consent (to registry participation), provided the research use of health information satisfies certain regulatory conditions. In addition, the Privacy Rule created Privacy Boards specifically to approve waivers of authorization for the research use of health information in organizations without an IRB.[98] Waivers are discussed in detail below.

In certain limited circumstances, research subjects can consent to future unspecified research using their identifiable patient information. The Common Rule permits an IRB-approved consent process to be broader than a specific research project[99] and to include information about research that may be done in the future. In its review of such future research, an IRB can subsequently determine that the previously obtained consent (1) satisfies or (2) does not satisfy the regulatory requirements for informed consent. If the previously obtained consent is not satisfactory, an additional consent process may be required; alternatively, the IRB may grant a waiver of consent, provided the regulatory criteria for a waiver are satisfied.

As such, an IRB-approved consent process for the creation of a research registry should include a description of the specific types of research to be conducted using registry data. For any future research that involves private identifiable information maintained by the registry, the IRB may determine that the original consent process (for the creation of the research registry) satisfies the applicable regulatory requirements because the prospect of future research and future research projects were adequately described. The specific details of that future research using registry data may not have been known when data were collected to create the registry, but that research may have been sufficiently anticipated and described to satisfy the regulatory requirements for informed consent. For consent to be informed as demanded by the ethical principle of respect for persons, however, any description of the nature and purposes of the research should be as specific as possible.

If a registry developer anticipates subsequent research use of identifiable private registry data, he or she should request an assessment by the IRB of the description of the research that will be used in the consent process for potential subjects at the time the data are initially collected. Nonetheless, in its review of any subsequent research, an IRB may require an additional consent process for each research subject or may grant a waiver for obtaining further consent.

Historically, HHS clearly rejected broadening the description of purpose in authorizations under the Privacy Rule to include future unspecified research.[100] As a result, the research purpose stated in an original authorization for a registry was limited to the use of registry data for that purpose.[101] However, under the modified HIPAA Privacy Rule released on January 25, 2013, HHS modified its prior

interpretation and guidance that research authorizations must be research study specific.[102] While this modification does not make any changes to the authorization requirements at 42 CFR § 164.508, HHS will no longer interpret the "purpose" provision for authorization requirements as study specific, thereby allowing future research to be authorized provided the authorization includes a description of the purpose of any future research.[103] Authorization of subsequent use of registry data maintained within a health care provider or insurance plan for a different future research purposes is now permitted, provided these additional uses or purposes are described to the extent that an individual could reasonably expect these future uses or disclosures of his or her PHI in the authorization from each individual whose registry data would be involved or an approved waiver of authorization is obtained. Alternatively, the use or disclosure of a limited dataset or de-identified registry data can occur, provided regulatory criteria are satisfied. Registries maintained by organizations to which the Privacy Rule does not apply (e.g., funding agencies for research that are not health care providers or insurance plans, professional societies, or non-health care components of hybrid entities such as universities) are not legally bound by the limited purpose of the original authorization. However, data sources or their business associates subject to the Privacy Rule are unlikely to be willing to provide patient information without a written agreement with the registry developer that includes legally enforceable protections against redisclosure of identifiable patient information. A valid authorization contains a warning to patients that their health information may not be protected by Privacy Rule protections in recipient organizations.[104]

Registry developers can request that patients obtain and share copies of their own records from their health care providers or insurance plans. This strategy can be useful for mobile populations, such as elderly retirees who occupy different residences in winter and summer, and for the health records of school children. A Federal privacy law[105] protects the health records of children that are held by schools from disclosure without explicit parental consent; thus, parents can often obtain copies of these records more easily than investigators. Alternatively, individuals can simply be asked to volunteer health information in response to an interview or survey. These collection strategies do not require obtaining a Privacy Rule authorization from each subject; IRB review and other requirements of the Common Rule, including careful protections of the confidentiality of registry data, may, nonetheless, apply to a registry project with a research purpose. Moreover, a registry developer may encounter Privacy Rule requirements for the use or disclosure of patient information by a health care provider or insurance plan for purposes of recruiting registry participants. For example, a patient authorization or waiver of authorization (discussed below) may be necessary for the disclosure of patient contact information by a health care provider or insurance plan (covered entity or their business associate) to a registry developer.

### 3.3.4. Certificates of Confidentiality and Other Privacy Protections

Certificates of confidentiality granted by the NIH permanently protect identifiable information about research subjects from legally compelled disclosure. For the purposes of certificates of confidentiality, identifiable information is broadly defined to include any item, or combination of items, in research data that could directly or indirectly lead to the identification of a research participant.[106] Federal law authorizes the Secretary of HHS (whose authority is delegated to NIH) to provide this privacy protection to subjects of biomedical, behavioral, clinical, and other research.[107] Federal funding for the research is not a precondition for obtaining a certificate of confidentiality.[108] An investigator whose research project has been granted a certificate of confidentiality may refuse to disclose identifying information collected for that research even though a valid subpoena demands that information for a civil, criminal, administrative, or legislative proceeding at the Federal, State, or local level. The protection provided by a certificate of confidentiality is intended to prevent the disclosure of personal information that could result in adverse effects on the social, economic, employment, or insurance status of a research subject.[109] Detailed information about certificates of confidentiality is available on the NIH Web site.[110]

The grant of a certificate of confidentiality to a research project, however, is not intended to affect State laws requiring health care and other professionals to report certain conditions to State officials; for example, designated communicable diseases, neglect and abuse of children and the elderly, or threats of violent harm. If investigators are mandatory reporters under State law, in general, they continue to have a legal obligation to make these reports.[111] In addition, other limitations to the privacy protection provided by certificates of confidentiality exist and may be relevant to particular research projects. Information on the NIH Web site describes some of these other legal limitations.[112]

Registry developers should also be aware that Federal law provides specific confidentiality protections for the identifiable information of patients in drug abuse and alcoholism treatment programs that receive Federal funding.[113] These programs may disclose identifiable information about their patients for research activities only with the documented approval of the program director and authorization of the patient.[114] The basis for the director's approval is receipt of written assurances about the qualifications of the investigator to conduct the research and the confidentiality safeguards incorporated into the research protocol, and an assurance that there will be no further disclosure of identifying information by the investigator. Moreover, an independent review of the research project should determine and verify in writing that the protocol provides adequate protection of the rights and welfare of the patients and that the benefits of the research outweigh any risks to patients.[115] Prior to submitting proposed consent documentation to an IRB, registry developers should consult legal counsel about the limitations of these confidentiality protections.

As a condition of approval, IRBs frequently require investigators to obtain a certificate of confidentiality for research involving information about substance abuse or other illegal activities (e.g., underage purchase of tobacco products), sexual attitudes and practices, and genetic information. Registry developers should consult legal counsel to determine if and how the limitations of a certificate of confidentiality may affect privacy protection planning for registry data. In all circumstances, the consent process should ensure that clear notice is given to research subjects about the extent of privacy protections they may expect for their health information when it is incorporated into a registry.

In the absence of a certificate of confidentiality, a valid subpoena or court order for registry data will usually compel disclosure of the data unless State law specifically protects the confidentiality of data. For example, Louisiana's laws specifically protect the collection of information related to tobacco use from subpoena.[116] On the other hand, a subpoena or court order may supersede State law confidentiality protections. These legal instruments can be challenged in the court having jurisdiction for the underlying legal proceeding. In some circumstances, research institutions may be willing to pursue such a challenge. The remote yet definite possibility of this sort of disclosure should be clearly communicated to research subjects as a limitation on confidentiality protections, both during the consent process and in an authorization for use or disclosure of patient information.

State law may assure the confidentiality of certain quality I/A activities performed by health care providers as peer review activities.[117] When State law protects the confidentiality of peer review activities, generally, it is implementing public policy that encourages internal activities and initiatives by health care providers to improve health care services by reducing the risks of medical errors and systematic failures. Protection by peer review statutes may limit the use of data generated by quality I/A activities for any other purposes.

### 3.3.5. Waivers and Alterations of Authorization and Consent

As mentioned above, the Privacy Rule authorizes Privacy Boards and IRBs to sometimes waive or alter authorizations by individual patients for the disclosure or use of health information for research purposes. (See Case Example 13.) In addition, the Common Rule authorizes IRBs to waive or alter the consent process. It is important for registry developers to keep distinct the terms "consent" and "authorization," as they are not interchangeable with respect to the Privacy Rule and Common Rule. As described above, authorization is the term used to describe permission required by the Privacy Rule and consent is the term used to describe permission required by the Common Rule. There are separate requirements for each of these permissions.

The Privacy Rule and the Common Rule each specify the criteria under which waivers or alterations of authorization and the consent process are permitted.[118] There are potential risks to patients participating in the registry resulting from these waivers of permission. A waiver of authorization potentially imposes the risk of a loss of confidentiality and consequent invasion of privacy. A waiver of consent potentially imposes risks of harm from the loss of self-determination, dignity, and privacy expected under the ethical principles of respect for persons and beneficence. Acknowledging these potential risks, regulatory criteria for waiver and alterations require an IRB or Privacy Board to determine that risks are minimal, in addition to other criteria. This determination is a necessary condition for approval of an investigator's request for a waiver or alteration of these permissions.

The following discussion refers only to waivers; registry developers should note that Privacy Boards and IRBs may approve alterations to authorizations or the consent process, provided a requested alteration satisfies all the same criteria required for a waiver by the Privacy Rule or Common Rule. Alterations are generally preferable to waivers in an ethical analysis based on the principle of respect for persons, because they acknowledge the importance of self-determination. In requesting alterations to an authorization or to the consent process, registry developers should be prepared to justify each proposed change or elimination of required elements (such as description of alternative procedures, courses of treatment, or benefits). Plausible justifications include a registry to which a specific element does not apply or a registry in which one element contradicts other required information in the authorization or consent documentation. The justifications for alterations should relate as specifically and directly as possible to the regulatory criteria for IRB or Privacy Board approval of waivers and alterations.

The Privacy Rule permits an IRB or Privacy Board to approve a waiver of authorization if the following criteria are met: (1) the use or disclosure involves no more than minimal risk to the privacy of individuals; (2) the research cannot be practicably conducted without the waiver; and (3) the research cannot be practicably conducted without access to, and use of, health information. The determination of minimal risk to privacy includes several elements: an adequate plan to protect identifiers from improper use or disclosure; an adequate plan to destroy identifiers, unless a health or research justification exists to retain them; and adequate written assurances that the health information will not be reused or disclosed to others, except as required by law, as necessary for oversight of the research, or as permitted by the Privacy Rule for other research.[119] The Privacy Board or IRB should provide detailed documentation of its decision to the health care provider or insurance plan (covered entity) that is the source of the health information for registry data.[120] The documentation should clearly communicate that each of the criteria for a waiver required by the Privacy Rule has been satisfied.[121] The Privacy Board or IRB documentation should also provide a description of the health information it determined to be necessary to the conduct of

the research and the procedure it used to approve the waiver.[122] A health care provider or insurance plan or their business associate may insist on legal review of this documentation before permitting the disclosure of any health information.

The criteria for a waiver of consent in the Common Rule are similar to those for a waiver of authorization under the Privacy Rule. An IRB should determine that: (1) the research involves no more than minimal risk to subjects; (2) the waiver will not adversely affect the rights and welfare of subjects; (3) the research cannot practicably be carried out without a waiver; and (4) whenever appropriate, subjects will be provided with additional information after participation.[123] The criterion for additional information can be satisfied at least in part by public disclosure of the purposes, procedures, and operations of a registry, as discussed in Section 4.1.

Some IRBs produce guidance about what constitutes "not practicable" justifications and the circumstances in which justifications remain are applicable. For population-based research projects, registry developers may also present the scientific justification of avoiding selection bias. A waiver permits the registry to include the health information of all patients who are eligible. An IRB may also agree to consider requests for a limited waiver of consent that applies only to those individuals who decline use of their health information in a registry project. This limited waiver of consent most often permits the collection of de-identified and specified information sufficient to characterize this particular population.

An important difference between the Common Rule and FDA regulations for the protection of human subjects involves consent to research participation. The FDA regulations require consent, except for emergency treatment or research, and do not permit the waiver or alteration of informed consent.[124] If registry data are intended to support the labeling of an FDA-regulated product, a registry developer should plan to obtain the documented, legally effective, voluntary, and informed consent of each individual whose health information is included in the registry.

The Common Rule also permits an IRB to waive documentation of the consent process under two different sets of regulatory criteria. The first set of conditions for approval of this limited waiver requires that the only record linking an individual subject to the research is the consent document, and that the principal risk to subjects is the potential harm from a breach of confidentiality. Each subject individually determines whether his or her consent should be documented.[125] Alternatively, an IRB can waive documentation of consent if the research involves no more than minimal risk of harm to subjects and entails no procedures for which written consent is normally obtained outside of a research context.[126] For either set of regulatory criteria, the IRB may require the investigator to provide subjects with written

information about the research activities in which they participate.[127] The written information may be as simple as a statement of research purposes and activities, or it may be more elaborate, such as a Web site for regularly updated information describing the progress of the research project.

The Privacy Rule creates a legal right for patients, by request, to receive an accounting of certain disclosures of their health information that are made by health care providers and insurance plans.[128] The accounting must include disclosures that occur with a waiver of authorization approved by a Privacy Board or IRB. The Privacy Rule specifies the information that an accounting should contain[129] and requires it to cover a six-year period or any requested shorter period of time.[130] If multiple disclosures are made to the same recipient for a single purpose, including a research purpose, a summary of these disclosures may be made. In addition, because most waivers of authorization cover records of many individuals, and thus an individualized accounting in such circumstances may be burdensome or impossible, the Privacy Rule provides that if the covered entity has disclosed the records of 50 or more individuals for a particular research purpose, the covered entity may provide to the requestor a more general accounting, which lists the research protocols for which the requestor's information may have been disclosed, among other items.[131]

### 3.3.6. Patient Safety Organizations

The final rule (the "Rule") implementing the Patient Safety and Quality Improvement Act of 2005 (PSQIA) became effective on January 19, 2009.[132] The PSQIA was enacted in response to a 1999 report by the Institute of Medicine that identified medical errors as a leading cause of hospital deaths in the United States, with many such errors being preventable.[133] The PSQIA allows health care providers to voluntarily report patient safety data, known as patient safety work product (PSWP), to independent patient safety organizations (PSOs). In general, PSWP falls into three general categories: (1) information collected or developed by a provider for reporting to a PSO and actually reported; (2) information developed by the PSO itself as part of patient safety activities; and (3) information that identifies or constitutes the deliberations or analysis of, or identifies the fact of reporting to, a patient safety evaluation system.[134] The PSQIA broadly defines PSWP to include any data, reports, records, memoranda, analyses, and statements that can improve patient safety, health care quality, or health care outcomes, provided that all such data must be developed for the purpose of reporting it to a PSO. Certain categories of information are expressly excluded from being PSWP. These include "a patient's medical record, billing and discharge information, or any other original patient or provider information...[and] information that is collected, maintained, or developed separately, or exists separately, from a patient safety evaluation system."[135]

Once PSWP is collected by a PSO, it is aggregated and analyzed by the PSO to assist a provider in determining, among other things, certain quality benchmarks and underlying causes of patient risks. Under the PSQIA, PSWP is considered privileged and confidential. Once PSWP is transmitted from the provider to the PSO, it may not be disclosed unless certain requirements are met. Penalties may be imposed for any breaches.[136]

However, PSOs may disclose PSWP—that is, they may release, transfer, provide access to, or otherwise divulge PSWP to another person—as long as it is an authorized disclosure under the PQIA and its Rule by meeting one or more exceptions. These exceptions include disclosures authorized by the identified health care providers and disclosures of nonidentifiable PSWP and disclosures to FDA, among others.[137] With respect to disclosure of PSWP for purposes of research, the regulations provide a very narrow exception. The Rule allows for disclosure of identifiable PSWP to entities carrying out "research, evaluations or demonstration projects that are funded, certified or otherwise sanctioned by rule or other means by the Secretary [of Health and Human Services]."[138] All such disclosures must comply with HIPAA as well as the PSQIA. Notably, the disclosure of PSWP for general research activities is not permitted under the PSQIA or the Rule.

An organization desiring to become a PSO must complete and submit a certification form to AHRQ to become "listed" as a PSO.[139] A registry may choose to become listed as a PSO; however, the registry should consider whether the obligations imposed on it in its capacities as a PSO would limit or otherwise restrict its attainment of its original objectives and whether it can fully meet the requirements of the PSQIA. In particular, PSO activities give rise to a business associate arrangement triggering Privacy Rule requirements.[140] In evaluating whether or not to be listed as a PSO, the registry developer should carefully review the registry's organizational structure and data collection processes to help ensure that there is a clear distinction between the collection of registry-related data and PSWP. For example, certain registries may publish certain information and results related to the data collected in the registry. As described above, if that registry is a PSO, then it must ensure that any data published do not constitute unauthorized disclosure for purposes of the PSQIA or HIPAA. It is important that an applicable exception to the disclosure of PSWP exist. Instead of becoming a PSO itself, a registry may elect to form a separate division or legal organization that it controls. These types of PSOs are referred to as "Component PSOs." This structure may help segregate registry data and PSWP, thus reducing the possibility of an impermissible disclosure of PSWP.

## 3.4. Developments Affecting the Privacy Rule

### 3.4.1. The Institute of Medicine Report

On February 4, 2009, the Institute of Medicine (IOM) published a report that examined how research was being conducted within the framework of the Privacy Rule. Within the IOM Report were findings of the IOM Committee on Health Research and the Privacy of Health Information (the IOM Committee)—the group that had assessed whether the Privacy Rule had had an impact on the conduct of health research. This group had proposed recommendations to ensure that important health research might be conducted while maintaining or strengthening privacy protections for research subjects' health information.[141] The IOM Report specifically acknowledged that the Privacy Rule was difficult to reconcile with other regulations governing the conduct of research, including the Common Rule and the FDA regulations, and it noted a number of inconsistencies among applicable regulations related to the de-identification of data and the use of informed consent for future research studies, among others.

Citing more uniform regulations in other countries, the IOM Report affirmed that "a new direction is needed, with a more uniform approach to patient protections, including privacy, in health research."[142] As its primary recommendation, the IOM Committee held that research should be entirely exempt from the Privacy Rule. In making such a recommendation, the IOM Committee encouraged Congress to allow HHS and other Federal agencies to develop separate guidance for the conduct of health research. Until such an overhaul could be accomplished, the IOM Committee called upon HHS to revise the Privacy Rule and associated guidance. HHS addressed some of these issues in the January 25, 2013 modifications to the Privacy Rule, such as allowing a broader interpretation of the "purpose" requirement for informed consent and incorporating PSO activities into the definition of activities giving rise to a business associate arrangment regulated by the Privacy Rule. Nevertheless, registry operators should be aware that additional modifications to the Privacy Rule as it relates to research activities may continue to be made.

### 3.4.2. The Genetic Information Nondiscrimination Act of 2008

The Genetic Information Nondiscrimination Act of 2008 (GINA) was signed into law on May 21, 2008. In general, GINA prohibits discrimination in health insurance coverage (Title I) and employment (Title II) based on genetic information. GINA defines genetic information as information about an individual's genetic tests, the genetic tests of an individual's family members, and the manifestation of a disease or disorder in an individual's family (e.g., family history). Title I of GINA took effect for most health insurance plans on May 22, 2009, and Title II became effective for employers on November 21, 2009. GINA also specifies that the definition of genetic information includes the genetic information of a fetus carried by a pregnant woman and an embryo legally held by an individual or family member utilizing an

assisted reproductive technology. Pursuant to GINA, health insurers and employers are prohibited from using the genetic information of individuals or their family members in determining health insurance eligibility and coverage, or in underwriting and premium setting, and employers from using genetic information in making employment-related decisions.

In addition to its nondiscrimination requirements, GINA also amended the Privacy Rule to clarify that genetic information is included within the Privacy Rule definition of protected health information. As a result, health plans and employers that are covered entities are required to treat any genetic information they collect as protected health information.[143]

### 3.4.3. The HITECH Act

The American Recovery and Reinvestment Act of 2009 (ARRA) was signed into law on February 17, 2009. Funds appropriated as a result of passage of ARRA are supporting new registries developed to study comparative effectiveness of treatments and protocols. It should be noted that there are no regulatory or ethical exceptions for such comparative effectiveness registries. Title XIII of ARRA, the Health Information Technology for Economic and Clinical Health Act (HITECH Act) significantly modified the rights and obligations of health care providers as covered entities and those who perform certain services on behalf of covered entities (their so-called *business associates*) as defined in the HIPAA Privacy Rule.

Perhaps most significantly, the HITECH Act extends to business associates many of the key privacy and security obligations contained in the Privacy Rule. Specifically, business associates are required to comply with security obligations such as administrative, physical, and technical safeguards, and documentation of these safeguards. While many business associate agreements previously contained general safeguarding requirements (e.g., requiring the business associate to maintain appropriate technical safeguards), these agreements often had not imposed specific security requirements (e.g., a requirement that the business associate implement procedures to terminate an electronic session after a predetermined time of inactivity). These expanded obligations now subject business associates to civil and criminal penalties that were once reserved only for covered entities under the Privacy Rule. The obligations imposed on business associates took effect on February 17, 2010, were finalized through HHS rulemaking on January 25, 2013, and will be effective on September 23, 2013.[144]

The HITECH Act also created a new requirement for covered entities and business associates to report data security breaches of the security or privacy of protected health information. If unsecured protected health information is accessed, acquired, used, or disclosed as a result of a data security breach, a covered entity must notify each individual whose information was improperly accessed, acquired, used, or

disclosed. Depending on the number of affected individuals, such notifications may be made via first-class mail, e-mail, posting on the entity's Web site, or by notice to media outlets.

If any unsecured protected health information stored or maintained by a business associate is breached or compromised, the business associate must provide notification to the applicable covered entity without unreasonable delay, and in no case later than 60 days after the breach becomes known, or reasonably should have become known, to the business associate. Any notification by a business associate must include the identification of any individual(s) whose information was accessed, acquired, or disclosed during the breach. Under the Privacy Rule, business associate agreements would contain similar breach notification requirements; however, the HITECH Act imposes a statutory obligation on business associates. The data breach notification requirements became effective September 23, 2009 and additional changes included in the new rules became effective on January 25, 2013.[145]

### 3.4.4. Summary of Regulatory Requirements

The use and disclosure of health information by health care providers and insurance plans and their business associates for research purposes, including registries, *are assumed* by the authors of this chapter to be subject to regulation under the Privacy Rule and *may* be subject to the Common Rule.

In general, the Privacy Rule permits the use by or disclosure of patient information to a registry, subject to specific conditions, in the following circumstances: (1) registries serving public health activities, including registries developed in connection with FDA-regulated products; (2) registries developed for the health care operations of health care providers and insurance plans (covered entities), such as quality I/A; (3) registries created by health oversight authorities for health system oversight activities authorized by law; (4) registries using de-identified health information; (5) registries using a "limited dataset" of patient information that lacks specified direct identifiers; (6) registries using information obtained with patient authorizations; or (7) registries using information obtained with a waiver or alteration of authorization.

The Common Rule will apply to the creation and use of registry data if (1) the organization where the registry resides is subject to Common Rule requirements or has an FWA that encompasses the registry project; *and* (2) the creation of the registry and subsequent research use of the registry data constitute non-exempt human subject research as defined by the Common Rule and are not exempt from Common Rule requirements; *and* (3) registry activities include a research purpose, which may be in addition to the main purpose of the registry. Registry developers are strongly encouraged to consult the IRB, not only about the applicability of the Common Rule, but also about the selection of data elements, the content of

the consent process or the regulatory criteria for waiver, and any anticipated future research involving identifiable registry data.

State laws regulate public health activities and may also apply in various ways to the research use of health information. NIH can issue certificates of confidentiality to particular research projects for the protection of identifiable personal information from most legally compelled disclosures. Federal law provides specific privacy protections to the health information of patients in substance abuse programs that receive Federal funding. The institutional policies of health care providers and insurance plans may also affect the use and disclosure of the health information of their patient or insured populations.

Legal requirements applying to use or disclosure of health information for research are evolving and can significantly influence the planning decisions of registry developers and investigators. It is prudent to obtain early and frequent consultation, as necessary, with institutional privacy officers, Privacy Board, or IRB staff and members, information system representatives of health care providers and insurance plans, plus technology transfer representatives and legal counsel.

# 4. Registry Transparency, Oversight, and Data Ownership

## *4.1. Registry Transparency*

Efforts to make registry operations transparent (i.e., to make information about registry operations public and readily accessible to anyone who is interested) are desirable. Such efforts may be crucial to realizing the potential benefits of research using health information. Registry transparency can also educate about scientific processes. Transparency contributes to public and professional confidence in the scientific integrity and validity of registry processes, and therefore in the conclusions reached as a result of registry activities. Public information about registry operations may also increase the scientific utility of registry data by promoting inquiries from scientists with interests to which registry data may apply.

Registry developers can promote transparency by making the registry's scientific objectives, governance, eligibility criteria, sampling and recruitment strategies, general operating protocol, and sources of data available to anyone who is interested. Proprietary interests of funding agencies, contractual obligations, and licensing terms for the use of patient or claims information may limit, to some extent, the information available to the public about the registry. It is important to stress that, while transparency and access to information are to be encouraged, the intent is not to discourage or criticize investments in patient registries that produce proprietary information. Neither the funding source nor the generation of proprietary information from a registry determines whether a registry adheres to the good practices

described in this handbook. Funding agencies, health care providers, and insurance plans do, however, have an important stake in maintaining public confidence in how health information is managed. The extent of registry transparency should be prospectively negotiated with these entities.

Creating a Web site of information about registry objectives and operations is one method of achieving transparency; ideally, registry information should be available in various media. An IRB may require registry transparency as a condition of approval to satisfy one of the regulatory criteria for granting a waiver of consent, which is to provide "additional pertinent information after participation."[146] For those interested, a useful example of registry transparency can currently be found on an international transplant registry Web site.[147]

## 4.2. Registry Oversight

Registry governance must reflect the nature and extent of registry operations. As described in Chapter 2, governing structures can vary widely, from one in which the registry developer is the sole decisionmaker to a system of governance by committee(s) comprised of representatives of all stakeholders in the registry, including investigators, the funding agency, patients, clinicians, biostatisticians, information technology specialists, and government agencies.

Registry developers should also consider appointing an independent advisory board to provide oversight of registry operations. An advisory board can assist registry operations in two important ways: (1) providing guidance for the technical aspects of the registry operations, and (2) establishing the scientific independence of the registry. The latter function can be valuable when controversies arise, especially those related to patient safety and treatment, or resulting from actions by a regulatory agency. Advisory boards collectively should have relevant technical expertise, but should also include representatives of other registry stakeholders, including patients. Advisory board actions should be limited to making recommendations to the ultimate decisionmaker, whether an executive committee or the registry developer.

Registry developers may also appoint other types of oversight committees to resolve specific recurring problems, such as verifying diagnoses of patient conditions or adjudicating data inconsistencies.

## 4.3. Data Ownership

### 4.3.1. Health Information Ownership in General

Multiple entities are often in a position to assert ownership claims to health information in various forms. Certain States have enacted laws that assign ownership of health records.[148] The Privacy Rule was not

intended to affect existing laws governing the ownership of health records.[149] At the current time, such claims of ownership are plausible, but none is known to be legally tested or recognized, with the exception of copyright. Entities that could claim ownership include health care providers and insurance plans, funding agencies for registry projects, research institutions, and government agencies. Notably, health care providers are required by State law to maintain documentation of the services they provide. This documentation is the medical-legal record compiled on each patient who receives health care services from an individual or institutional provider. Individuals, including patients (who may have a potential liberty interest in maintaining control of its use), registry developers, and investigators, may also assert ownership claims to health information. The basis for these claims is control of the tangible expression of and access to the health information.

There is no legal basis for assertions of ownership of facts or ideas; in fact, established public policy supports the free exchange of ideas and wide dissemination of facts as fundamental to innovation and social progress.[150] However, as a tangible expression of health information moves from its creation to various derived forms under the control of successive entities, rights of ownership may be transferred (assigned), shared, or maintained, with use of the information under a license (i.e., a limited transfer of rights for use under specific terms and conditions). Currently, in each of these transactions, the rights of ownership are negotiated on a case-by-case basis and formalized in written private agreements. The funding agency for a registry may also assert claims to ownership as a matter of contract law in their sponsorship agreements with research organizations.

Many health care providers are currently installing systems for electronic health records at great expense. Many are also contemplating an assertion of ownership in their health records, which may include ownership of copyright. The claim to ownership by health care providers may be an overture to commercialization of their health care information in aggregate form.[151] Public knowledge of and response to such assertions of ownership are uncertain at this time. A licensing program for the use of health information may enable health care providers to recoup some of their investment costs of electronic health records including the expenses associated with the technicians engaged to maintain them. In the near future, research use of health information for a registry may require licensing, in addition to the terms and conditions in data use agreements and, if necessary, in business associate agreements required by Privacy Rule regulations. Subsequent research use of the registry data will likely be based on the terms of the original license.

Among the changes ARRA has made in the regulation of health care information is a prohibition on its sale, subject to certain exceptions, including one for research use. This exception permits covered entities to recover reasonable payment for processing of health information for research use.[152]

For academic institutions, publication rights are an important component of intellectual property rights in data. Formal institutional policies may address publication rights resulting from faculty educational and research activities. Moreover, the social utility and benefit of any registry is evaluated on the basis of its publicly known findings and any conclusions based on them. The authors strongly encourage registry developers to maximize public communication of registry findings through the customary channels of scientific conferences and peer-reviewed journals. The goal of public communication for scientific findings and conclusions applies equally to registries operated outside of academic institutions (i.e., directly by industry or professional societies). For further discussion of developing data access and publication policies for registries, see Chapter 2.

The concept of ownership does not fit comfortably in the context of health information, because it largely fails to acknowledge individual patient privacy interests in health information. An inescapable personal nexus exists between individuals and information about their health. A recent failure that illustrates this relationship, with regard to patient interests in residual tissue from clinical procedures, resulted in widely publicized litigation to determine who owned the residual tissue and how it could be used for future research.[153] The legal concept of custody may be a useful alternative to that of ownership. Custodians have legal rights and responsibilities; for instance, those that a guardian has for a ward or parents have for their children. Custody also has a protective function, consistent with public expectations of confidentiality practices that preserve the privacy and dignity of individual patients. Custody and its associated legal rights and responsibilities are transferable from one custodian to another. The concept of custody can support health care provider investments in information systems and the licensed use of health information for multiple, socially beneficial purposes without denying patient interests in their health information.

The sharing of registry data subsequent to their collection currently presents special ethical challenges and legal issues.[154] The criteria used to determine the conditions for shared use include applicable Federal or State law as well as the regulatory requirements in place when the health information was originally obtained. These legal and regulatory requirements, as well as processing and licensing fees, claims of property rights, and concerns about legal liability, are likely to result in formal written agreements for each use of registry data. Moreover, to educate patients and to establish the scientific independence of the registry, registry developers should make known the criteria under which data is used.

Currently, there are no widely accepted social or legal standards that govern property rights in health information, with the possible exception of copyright, which is discussed below. At the time of this writing, health information sources and other users privately reach agreement to manage access and control. The Privacy Rule regulates the use and disclosure of health information by covered entities (certain health care providers and insurance plans), plus certain third parties working on behalf of covered entities, but does not affect current laws, if any, regarding property rights in health information when they exist.[155]

### 4.3.2. Copyright Protection for Health Information Registries

In terms of copyright theory, a health information registry is likely to satisfy the statutory definition of a compilation[156] and reflect independent creativity by its developer.[157] Thus, copyright law may provide certain protections for a health information registry existing in any medium, including electronic digital media. The "facts" compiled in a health information registry, however, do not correlate closely to other compilations protected by copyright, such as telephone books or even genetic databases.[158] Instead, registry data constitute legally protected, confidential information about individual patients to which independent and varied legal protections apply. Copyright protections may marginally enhance, but do not diminish, other legal restrictions on access to and use of health information and registry data. For more information on copyright law, see Appendix B.

## 5. Conclusions

Ethical considerations arise in many of the essential aspects of planning and operating a registry. These considerations can affect the scientific, logistical, and regulatory components of registry development, as well as claims of property rights in health information. The guiding ethical principles for these considerations are *respect for persons*, *beneficence*, and *justice*.

At the most fundamental level, investigations that involve human subjects and that are not capable of achieving their scientific purpose are unethical. The risk-benefit ratio of such studies is unacceptable in an analysis based on the principle of *beneficence*, which obligates investigators to avoid harming subjects, as well as maximizing the benefits and minimizing the harms of research projects. Ethical scientific design must be robust, must be based on an important question, and must ensure sufficient statistical power, precise eligibility criteria, appropriately selected data elements, and adequately documented operating procedures and methodologies.

In addition, an ethical obligation to minimize harms requires planning for and establishing adequate protections to ensure the confidentiality of the health information disclosed to a registry. Such planning

should include devising physical, technical, and administrative safeguards for access to and use of registry data. Reducing the potential harms from the use of health information in a registry is particularly important, because generally no directly offsetting benefit from participation in a registry accrues to individuals whose health information is used in the registry. According to an analysis applying the principle of *justice*, research activities that produce a significant imbalance of potential risks and benefits to participating individuals are unethical.

Protection of the confidentiality of the health information used to populate a registry reflects the ethical principle of *respect for persons and avoidance of harm*. Health information intimately engages the privacy and dignity of patients. Registry developers should acknowledge public expectations of protection for patient privacy and dignity with clear and consistent communications to patients about protections in place to prevent inappropriate access to and use of registry data.

The regulatory requirements of the Privacy Rule and Common Rule have deep connections to past ethical concerns about research involving human subjects, to general social anxiety about privacy associated with rapid advances in health information systems technology and communications, and to current biomedical developments in human genetics. Compliance with these regulatory requirements not only is a cost of doing business for a registry project, but also demonstrates recognition of the ethical considerations accompanying use of health information for scientific purposes. Compliance efforts by registry developers also acknowledge the important public relations and liability concerns of health care providers and insurance plans, public health agencies, health oversight agencies, and research organizations. Regulatory compliance contributes to, and generally supports, the credibility of scientific research activities and research organizations, as well as that of particular projects.

Federal and State privacy laws may affect registry development, especially registries created for public health purposes. These laws express an explicit, legislatively determined balance of individual patient interests in health information against the potential social benefits from various uses of that information, including in research. Consultation with legal counsel is strongly recommended to determine the possible effect of these laws on a particular registry project.

Ethical considerations also affect the operational aspects of registries, including governance, transparency, and data ownership. Registry governance, discussed in Chapter 2, should reflect both appropriate expertise and representation of stakeholders, including patients. An independent advisory committee can provide useful guidance to registry developers and managers, especially on controversial issues. Transparency involves making information about registry governance and operations publicly available. Registry transparency improves the credibility of the scientific endeavors of a registry, the use

of health information for scientific purposes, and the results based on analyses of registry data. In short, registry transparency promotes public trust.

Claims of "ownership" of health information and registries are plausible, but have not yet been legally tested. In addition, how the public would respond to such claims is uncertain. Ostensibly, such claims do not seem to acknowledge patient interests in health information. Nonetheless, in theory, copyright protections for compilations may be applied to the patient information held by health care providers and insurance plans, as well as to registries. In general, property rights related to health information are likely to be negotiated privately under the terms and conditions of formal agreements between registry developers, funding agencies, and health care providers or insurance plans. As a practical matter, "ownership" implies operational control of registry data and publication rights.

In summary, careful attention to the ethical considerations associated with the design and operation of a registry, and fulfillment of the applicable legal requirements, are critical to the success of registry projects and to the realization of their social and scientific benefits.

## 6. Summary of Privacy Rule and Common Rule Requirements

Table 1 summarizes Privacy Rule and Common Rule requirements. The table generally assumes that the Privacy Rule applies to the data source— i.e., that the data source is a "covered entity" or their "business associate." The exception is Category 8, registry developers that use data not subject to the Privacy Rule.

Note that the information in the table is a simplified summary of material that is or may become subject to other laws and to individual institutional policies. Each research project is unique. Therefore, this table is not intended to provide answers to specific questions that arise in the context of a given project. This table is no substitute for consultation with institutional officials and others about the regulatory requirements that apply to a particular registry project.

**Table 1. Summary of Privacy Rule and Common Rule Requirements**

| Registry developer or purpose of registry | Health information is de-identified* | Health information excludes direct identifiers | Health information includes direct identifiers | Waiver of authorization, documentation of consent, or consent process |
|---|---|---|---|---|
| 1A. Federal or State public health agency: Registry for *public health practice within agency's legal authority* **not** *involving research.* | No requirements. | The Privacy Rule permits use or disclosure to a public health authority for public health activities.<br>The Common Rule is not applicable. | The Privacy Rule permits use or disclosure to a public health authority for public health activities.<br>The Common Rule is not applicable. | Waivers are not applicable. |
| 1B. Federal or State public health agency: Registry is an agency *research project*. | No requirements. | The Privacy Rule permits the use or disclosure of limited dataset, provided the data source and registry developer enter into a DUA.<br>The Common Rule may apply.** | The Privacy Rule permits use or disclosure with patient authorization or IRB or Privacy Board waiver of authorization.<br>If the Common Rule applies,** IRB review and documented consent are required, unless an IRB grants a waiver of documentation or waiver for the consent process. | Privacy Board or IRB approval of a waiver of authorization depends on satisfaction of specific regulatory criteria.<br>If the Common Rule applies,** IRB approval of a waiver of consent documentation or process depends on satisfaction of specific regulatory criteria. |
| 2. Registry producing evidence in support of labeling for an *FDA-regulated product*. | No requirements. | The Privacy Rule permits use or disclosure to a person responsible for an FDA-regulated product.<br>The Common Rule may apply.** | The Privacy Rule permits use or disclosure to a person responsible for an FDA-regulated product.<br>FDA regulations, and Common Rule, if applicable,** require IRB review, a documented consent | Waivers are not applicable.<br>If the Common Rule applies,** IRB approval of a waiver of consent documentation or process depends on satisfaction of specific regulatory criteria. |

| **Registry developer or purpose of registry** | **Health information is de-identified*** | **Health information excludes direct identifiers** | **Health information includes direct identifiers** | **Waiver of authorization, documentation of consent, or consent process** |
|---|---|---|---|---|
| | | | process, and protection of confidentiality of research data. | |
| 3. Health oversight agency registry to perform *a health oversight activity* **not** *involving research.* | No requirements. | The Privacy Rule permits use or disclosure for health oversight activities authorized by law.<br>The Common Rule is not applicable. | The Privacy Rule permits use or disclosure for health oversight activities authorized by law.<br>Institutional policy may apply the Common Rule or require IRB review. | Waiver of authorization is not applicable.<br>If institutional policy applies the Common Rule, IRB approval of a waiver of consent documentation or process depends on satisfaction of specific regulatory criteria. |
| 4. *Registry required by law*; Common Rule may apply if registry *involves research.* | No requirements. | The Privacy Rule permits use or disclosure required by other law.<br>If the Common Rule applies,** it permits an IRB grant of exemption if the data is existing or publicly available, unless a re-identification code is used.<br>The Common Rule may apply, however the study may qualify for exemption. | The Privacy Rule permits use or disclosure required by other law.<br>The Common Rule may apply, however the study may qualify for exemption. Institutional policy may apply the Common Rule or require IRB review whether or not a research purpose is involved. | Waiver of authorization is not applicable.<br>If the Common Rule applies,** IRB approval of a waiver of consent documentation or process depends on satisfaction of specific regulatory criteria. |
| 5. *Quality I/A registry* **not** *involving research.* | No requirements. | The Privacy Rule permits the use or disclosure of a limited dataset for health care operations, provided the data source and registry developer enter into a data use agreement. | The Privacy Rule permits use or disclosure for the "health care operations" of the data source and, in certain circumstances, of another covered entity. | Waivers are not applicable. |

| **Registry developer or purpose of registry** | **Health information is de-identified*** | **Health information excludes direct identifiers** | **Health information includes direct identifiers** | **Waiver of authorization, documentation of consent, or consent process** |
|---|---|---|---|---|
| | | The Common Rule is not applicable. | The Common Rule is not applicable. | |
| 6. Research registry residing in organization to which Common Rule applies.** | No requirements. | The Privacy Rule permits the use or disclosure of a limited dataset for research, provided the data source and registry developer enter into a DUA.<br>The Common Rule permits an IRB grant of exemption from review if the data is existing or publicly available, unless a re-identification code is used. | The Privacy Rule permits use or disclosure for research with individual patient authorization or an IRB or Privacy Board waiver of authorization.<br>The Common Rule requires IRB review and documented consent unless the IRB grants a waiver of documentation of consent or a waiver for the consent process. | IRB or Privacy Board approval depends on satisfaction of specific regulatory criteria. |
| 7. *Research registry* developed by organization that is not a health care provider or insurance plan and is not subject to the Common Rule, using health information obtained from a health care provider or insurance plan. | No requirements. | The Privacy Rule permits the disclosure of a limited dataset, provided the data source and registry developer enter into a DUA. | The Privacy Rule permits use or disclosure for research with individual patient authorization or waiver of authorization. | Privacy Board approval of a waiver of authorization depends on satisfaction of specific regulatory criteria. |
| 8. Research registry | No | No requirements. | No requirements. | Waivers are not applicable. |

| Registry developer or purpose of registry | Health information is de-identified* | Health information excludes direct identifiers | Health information includes direct identifiers | Waiver of authorization, documentation of consent, or consent process |
|---|---|---|---|---|
| developed by organization that is not a health care provider or insurance plan and is not subject to the Common Rule, using health information collected from entities not subject to the Privacy Rule. | requirements. | | | |

**Information lacks the data elements specified in the Privacy Rule standard for de-identification.*
***The Common Rule likely applies if: (1) Federal funding is involved with the registry project, (2) the organization within which the registry will reside has agreed in its Federalwide Assurance (FWA) to apply the Common Rule to all research activities conducted in its facilities or by its employees. Note that institutional policy may also apply the Common Rule.*
***Note:*** *Reference to this table is not a substitute for consultation with appropriate institutional officials about the regulatory requirements that may apply to a particular registry project. FDA = U.S. Food and Drug Administration. IRB = Institutional Review Board. DUA = Data Use Agreement.*

## Case Examples for Chapter 7

### Case Example 13. Obtaining a Waiver of Informed Consent

| | |
|---|---|
| **Description** | The TVT Registry™ tracks patient safety and real-world outcomes for patients undergoing a transcatheter aortic valve replacement (TAVR) procedure for treatment of aortic stenosis. The registry collects data on patient demographics, procedure details, and facility and physician information to support analyses of patient outcomes and clinical practice patterns. The Centers for Medicare & Medicaid Services (CMS) approved the registry as meeting the requirements outlined in the Medicare National Coverage Decision on TAVR. |
| **Sponsor** | The Society of Thoracic Surgeons (STS) and the American College of Cardiology (ACC) |
| **Year Started** | 2012 |
| **Year Ended** | Ongoing |
| **No. of Sites** | 247 hospitals |
| **No. of Patients** | 9,051 patients |

#### Challenge

Aortic stenosis is the most common valvular abnormality in the United States, and the prevalence of this condition is expected to increase as the U.S. population ages. Until recently, surgical aortic valve replacement has been the only effective treatment for adults with severe symptoms. The TAVR procedure is a new option for patients who are considered to be inoperable for conventional aortic valve replacement surgery, but there is a lack of evidence on long-term patient outcomes.

In 2012, CMS issued a Medicare National Coverage Decision for TAVR. Under the decision, CMS permits Medicare coverage for TAVR only when 1) the procedure is performed with a device approved by the U.S. Food and Drug Administration (FDA) consistent with labeled indications and any other FDA requirement; 2) the procedure is performed in facilities meeting certain requirements; and 3) when all patients undergoing the TAVR procedure are included in a national TAVR registry or participate in an approved clinical study. The national TAVR registry must consecutively enroll TAVR patients, accept all manufactured devices, follow patients for at least one year, and comply with all relevant regulations related to the protection of human research subjects. The National Coverage Decision specifically requires that the registry collect data on the following outcomes: stroke, all cause mortality, transient ischemic attacks (TIAs), major vascular events, acute kidney injury, repeat aortic valve procedures, and quality of life.

The development of a national registry to meet these requirements was challenging, particularly due to the need to collect at least one year of follow-up and quality of life data. The registry was expected to enroll hundreds of sites and thousands of patients, making it time-consuming, administratively cumbersome, and expensive to obtain local IRB approval for each site and informed consent for each patient.

#### Proposed Solution

The registry developers determined that the national TAVR registry was most likely to be successful if it collected data that was already routinely documented as part of the standard of care and was able to obtain a waiver of informed consent from a central institutional review board (IRB). To obtain a waiver of informed consent, the registry must meet all of the following four criteria, as documented in 45 CFR 46.116(d):

1. The research involves no more than minimal risk to the subjects;
2. The waiver or alteration will not adversely affect the rights and welfare of the subjects;
3. The research could not practicably be carried out without the waiver or alteration; and,
4. Whenever appropriate, the subjects will be provided with additional pertinent information after participation.

When designing the data collection instruments for the registry, the developers worked closely with surgeons and interventional cardiologists to understand which data are already collected. The developers were able to limit the registry data collection effort to data that are already collected routinely, thereby allowing registry data to be abstracted from the medical record with no data collected solely for the purposes of the registry. In particular, the registry developers carefully considered how to collect follow-up data and quality of life data without requiring the collection of information solely for the purposes of the registry.

Based on discussions with surgeons and interventional cardiologists, the developers determined that patients are seen for follow-up care routinely at 30 days and 1 year following the procedure. Published guidelines have established the use of the Kansas City Cardiomyopathy Questionnaire (KCCQ) to assess quality of life as a standard of care for TAVR patients at these follow-up visits. The registry was designed to use the data collected at these follow-up visits, including the KCCQ, to meet the requirements for collecting long-term outcomes and quality of life information.

### Results

The registry began collecting data in 2012 and has been approved by CMS as meeting the requirements of the Medicare National Coverage Decision. The ACC and STS, the institutions operating the registry, are considered the only entities engaged in research, while the participating sites are considered to be providing data only. The registry was approved only by the single IRB designated under the ACC/STS's Federalwide Assurance (FWA). Based on the registry protocol, the IRB determined that the ACC/STS are engaged in research on human subjects and granted a waiver of informed consent. The waiver of informed consent was awarded primarily because the participating sites are collecting and submitting information that is already documented in the medical record as part of the standard of care. As the registry operators, the ACC and STS submit data, including patient identifiers, to CMS as required by the National Coverage Decision. However, the ACC and STS only conduct research on a limited data set, and any research studies not covered by the protocol are submitted to the IRB for review.

Because the ACC and STS have IRB approval and a waiver of informed consent, and because the data are already collected as part of the standard of care, the individual sites participating in the registry do not

necessarily need to go through an IRB prior to enrolling in the registry. Some individual sites elect to submit the registry to their local IRB, in many cases because they intend to use the data that they collect for the registry in additional research studies. The local IRBs generally have reached the same conclusion as the central IRB. However, a local IRB may reach a different conclusion, perhaps due to differences in the data collection process at an individual site. For example, the data collection process at an individual site may provide an opportunity to consent the patient, in which case the IRB may not grant a waiver of informed consent. In these cases, the individual site will follow the advice of the local IRB.

### Key Point

Protecting the subjects whose data will be used is of the utmost importance when developing a registry. When developing a registry, sponsors should consider the planned data collection effort in the context of requirements for IRB review and informed consent. This approach may help the registry identify a strategy that protects patients' privacy without overburdening the participating sites.

### For More Information

STS/ACC TVT Registry. https://www.ncdr.com/TVT/Home/Default.aspx. Accessed September 4, 2013.

## References

[1] See, for example, Section III, Article 8, of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[2] 45 CFR 160.103: definition of health information; 45 CFR 46.102(f): definition of human subject.
[3] 45 CFR Part 46.
[4] Part C of Title XI of the Social Security Act, 42 USC §§ 1320d to 1320d-8 (2000), and section 264 of the Health Insurance Portability and Accountability Act of 1996, 42 USC §1320d-2 note (2000); 45 CFR Parts 160 and 164.
[5] American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009), Division A, Title XIII and Division B, Title IV, Health Information Technology for Economic and Clinical Health Act (HITECH Act) (codified at 42 U.S.C. § 17930, et seq).
[6] National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. Apr 181979. [Accessed June 30, 2010]. Available at http://www.hhs.gov/ohrp /humansubjects/guidance/belmont.htm.
[7] Public Law 93-348 (1974), Title II.
[8] Council for International Organizations of Medical Sciences. International Guidelines for Ethical Review of Epidemiological Studies (hereinafter CIOMS Guidelines) 1991. [Accessed June 24, 2010]. Available at http://www.cioms.ch/publications/guidelines/1991_texts_of_guidelines.htm. and noted to be under revision. See especially sections entitled General Ethical Principles and Informed Consent.
[9] Grant RW, Sugarman J. Ethics in human subjects research: do incentives matter? J Med Philos. 2004;29(6):717–38.
[10] CIOMS Guidelines, note 6, at paragraphs 11 and 12.
[11] Department of Health and Human Services, Office of the Inspector General. Recruiting human subjects: sample guidelines for practice. OEI-01-97-00196. Jun, 2000. p. 5.
[12] Department of Health and Human Services, Office of the Inspector General. Recruiting human subjects: sample guidelines for practice. OEI-01-97-00196. Jun, 2000. Appendix A.
[13] Physician Payments Sunshine Act, S.301, The House of Congress (2010).
[14] Massachusetts regulation 105 CMR 970.000 implement M.G.L. c. 111N, Pharmaceutical and Medical Device Manufacturer Conduct, as enacted under Chapter 305 of the Acts of 2008, An Act To Promote Cost Containment, Transparency and Efficiency in the Delivery of Quality Health Care.
[15] CIOMS Guidelines, note 6, at paragraphs 18–21.
[16] CIOMS Guidelines, note 6, at paragraph 26.
[17] See generally CIOMS Guidelines, note 6, at paragraph 43. See also the Patient Protection and Affordable Care Act of 2010, Sec. 1101.
[18] CIOMS Guidelines, note 6, at paragraph 40.
[19] See, for example, U.S. Department of Health and Human Services (HHS) regulations at 45 CFR Part 46; 21 CFR Parts 50 and 56 for research conducted in support of products regulated by the U.S. Food and Drug Administration (FDA); CRS Report Federal Protection for Human Research Subjects: An Analysis of the Common Rule and Its Interactions with FDA Regulations and the HIPAA Privacy Rule. Updated June 2, 2005.
[20] Regulations identical to 45 CFR 46 Subpart A apply to research funded or conducted by a total of 17 Federal agencies, some of which may also require additional legal protections for human subjects.
[21] The terms of the model Federalwide Assurance (FWA) are available from the Office for Human Research Protection in the U.S. Department of Health and Human Services. [Accessed June 24, 2010]. http://www.hhs.gov/ohrp/humansubjects/assurance/filasurt.htm.
[22] Office for Human Research Protection. Guidance on Research Involving Coded Private Information or Biological Specimens. Oct 16, 2008.

[23] 45 CFR Part 46, Subpart A.
[24] See, for example International Society for Pharmacoepidemiology (ISPE). Guidelines for Good Pharmacoepidemiology Practices (GPP). Pharmacoepidemiol Drug Safety. 2004 2005 August;14:589–95. on the essential elements of a protocol.
[25] Part C of Title XI of the Social Security Act, 42 USC §§ 1320d to 1320d-8 (2000), and section 264 of the Health Insurance Portability and Accountability Act of 1996, 42 USC § 1320d-2 note (2000); 45 CFR Parts 160 and 164.
[26] 45 CFR 160.102, Applicability, and 160.103, definitions of covered entity, health care provider, health plan, health care clearinghouse, and transaction.
[27] HITECH Act §13404(a); 45 C.F.R. § 164.104(b); 78 Fed. Reg. at 5591.
[28] 45 CFR 160.203.
[29] Maryland Health General Statute §. 4–303(b)(4).
[30] 45 CFR 160.103 defines both "disclosure" and "use" for the purposes of the Privacy Rule.
[31] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 78 Fed. Reg. 5566 (January 25, 2013) (to be codified at 45 CFR pts 160 and 164).
[32] HITECH Act §13404(a); 45 C.F.R. § 164.104(b); 78 Fed. Reg. at 5591.
[33] 45 CFR 164.501.
[34] 67 Fed Reg 53231, August 14, 2002.
[35] 45 CFR 46.102(d).
[36] U.S. Department of Health and Human Services (HHS), National Institutes of Health (NIH). Health services research and the HIPAA Privacy Rule. NIH Publication Number 05-5308, May 2005. See also HHS, NIH. Research repositories, databases, and the HIPAA Privacy Rule. NIH Publication Number 04-5489, January 2004.
[37] 45 CFR 164.512(b).
[38] 45 CFR 164.501.
[39] Centers for Disease Control and Prevention. HIPAA Privacy Rule and Public Health: Guidance from CDC and the U.S. Department of Health and Human Services. MMWR. 2003:52. (early release)
[40]45 CFR 164.512(a).
[41] 45 CFR 164.508(a).
[42] 45 CFR 164.514(e).
[43] 45 CFR 164.514(a)–(c).
[44] 45 CFR 164.528.
[45] 45 CFR 164.512(i)(1)(i).
[46] 21 CFR 65.111(a)(7).
[47] Centers for Disease Control and Prevention. Guidelines for Defining Public Health Research and Public Health Non-Research, revised October 4, 1999. [Accessed 30 June 2010]. http://www.cdc.gov/od/science/regs/hrpp/researchdefinition.htmGostin LO. Public health law: power, duty, restraint. Berkeley and Los Angeles, CA: University of California Press; New York: The Milbank Memorial Fund; 2000. pp. 126–127. (hereinafter Public Health Law). See also CIOMS Guidelines, note 6, Introduction, noting that epidemiological practice and research may overlap.
[48] Bellin E, Dubler NN. The quality improvement-research divide and the need for external oversight. Am J Public Health. 2001;91(9):1512–1517. (hereinafter Quality Improvement-Research Divide). Lindenauer PK, Benjamin EM, et al. The Role of the institutional review board in quality improvement: a survey of quality officers, institutional review board chairs, and journal editors. Am J Med. 2002;113(7):575–9. Lo B, Groman M. Oversight of quality improvement: focusing on benefits and risks. Arch Intern Med. 2003;163(12):1481–6.
[49] Office for Human Research Protections. [Accessed June 24, 2010]. http://www.hhs.gov/ohrp.

[50] National Institutes of Health. Health services research and the HIPAA Privacy Rule. Publication Number 05-5308, p. 2–3. See also 45 CFR 164.501 for the definition of health care operations.
[51] A copy of the HHS version of the "Common Rule," 45 CFR Part 46, subpart A, and additional subparts B, C, and D regarding vulnerable populations may be obtained on the Web site of the Office for Human Research Protection (OHRP) in the U.S. Department of Health and Human Services. Available at: http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.htm. Accessed June 24, 2010.
[52] A copy of the "Privacy Rule," 45 CFR Parts 160 and 164, may be obtained on the Web site of the Office for Civil Rights (OCR) in the U.S. Department of Health and Human Services. [Accessed June 24, 2010]. http://www.hhs.gov/ocr/hipaa/finalreg.html.
[53] The Common Rule as adopted by HHS contains special protections for certain defined "vulnerable" populations, i.e., women, human fetuses, neonates, prisoners, and children. See 45 CFR Part 46, Subparts B, C, D.
[54] American College of Epidemiology: Policy Statement on Sharing Data from Epidemiologic Studies. May2002. [Accessed June 24, 2010]. http://www.acepidemiology.org/policystmts/DataSharing.pdf.
[55] 45 CFR 46.102(d).
[56] Centers for Disease Control and Prevention. National Program of Cancer Registries (NPCR). Description of SEER program. [Accessed June 24, 2010]. http://www.cdc.gov/cancer/npcr/css .htmsectionIV.
[57] 45 CFR 164.512(b).
[58] Gostin LO, Lillienfeld DE, Stolley PD Foundations of epidemiology (revised) Oxford University Press; 1994. p. 104.See also Gostin LO, Public Health Law, note 43, at 114, Table 5
[59] 45 CFR 164.512(d)
[60] 45 CFR 164.512(d)(1).
[61] 45 CFR 164.512(b)(1)(iii).
[62] 45 CFR 46.102(d) and 45 CFR 164.501, respectively.
[63] 45 CFR 46.102(d).
[64] 45 CFR 164.501.
[65] National Institutes of Health, U.S. Department of Health and Human Services. Health services research and the HIPAA Privacy Rule. NIH Publication No. 04-5489. Jan2004. [Accessed June 24, 2010]. pp. 2–3. http://privacyruleandresearch.nih.gov/healthservicesprivacy.asp.
[66] 45 CFR 164.501.
[67] Centers for Disease Control and Prevention. Guidelines for Defining Public Health Research and Public Health Non-Research. Oct 41999. [Accessed June 30, 2006]. pp. 126–127. http://www .cdc.gov/od/ads/opspoll1.htm. Public Health Law, supra, note 43.See also CIOMS Guidelines, supra, note 6, Introduction, noting that epidemiological practice and research may overlap; and Quality Improvement-Research Divide, supra, note 44.
[68] Quality Improvement-Research Divide, note 44, 1512–7Lindenauer PK, Benjamin EM, et al. The role of the institutional review board in quality improvement: a survey of quality officers, institutional review board chairs, and journal editors. Am J Med. 2002;113(7):575–9.Lo B, Groman M Oversight of quality improvement: focusing on benefits and risks. Arch Intern Med. 2003;163(12):1481–6.
[69] See 45 CFR 160.103 for the definition of individually identifiable health information and 45 CFR 164.514(a)–(c) and (e) on the de-identification of health information and limited datasets, respectively.
[70] 45 CFR 46.102(f).
[71] 45 CFR 46.111(a)(7).
[72] 45 CFR 46.116(a)(5).
[73] See 45 CFR 164.514(a)–(c) and (e) on the deidentification of health information and limited datasets, respectively.
[74] 45 CFR 164.514(e)(2).
[75] 45 CFR 164.514(b).
[76] 45 CFR 164.514(b)(1).

[77] 45 CFR 164.514(c).
[78] FR vol 67 no 157, 53233, August 14, 2002
[79] 45 CFR 164.514(c).
[80] 45 CFR 46.102(f).
[81] 45 CFR 164.514(e)(2).
[82] 45 CFR 164.514(e)(4).
[83] 45 CFR 164.514(e)(4)(ii)(A).
[84] 45 CFR 164.514(e)(4)(ii)(C)(5).
[85] 67 Fed Reg 53181, 53236, August 14, 2002.
[86] 45 CFR 164.514(e)(2).
[87] 45 CFR 164.504(e).
[88] 45 CFR 164.504(e).
[89] 45 CFR 46.101(b)(4).
[90] 45 CFR 164.508.
[91] 45 CFR 164.508(c).
[92] 45 CFR 164.502(a)(1).
[93] 45 CFR 164.501.
[94] 45 CFR 46.102(f).
[95] 45 CFR 46.116.
[96] 45 CFR 164.508(b)(3).
[97] 45 CFR 46.116.
[98] 45 CFR 164.512(i)(1)(i)(B).
[99] 45 CFR 46.116.
[100] 67 Fed Reg 53181, 53226, August 14, 2002.
[101] Department of Health and Human Services. Institutional review boards and the HIPAA Privacy Rule. NIH Publication Number 03-5428. Aug2003. [Accessed June 24, 2010]. pp. 15–16. http://privacyruleandresearch.nih.gov/pdf/IRB_Factsheet.pdf.
[102] 45 C.F.R. § 164.508(b)(3); 78 Fed. Reg. at 5612.
[103] 45 C.F.R. § 164.508(c) and § 164.508(c)(1)(iv).
[104] 45 CFR 164.508(c)(2)(iii).
[105] Family Educational Rights and Privacy Act (FERPA), 20 USC 1232g, 34 CFR Part 99.
[106] From the NIH Web site.
[107] Public Health Services Act Section 301(d), 42 USC 241(d) as amended. See also 42 CFR Part 2a about research activities on mental health, including the use and effect of alcohol and other psychoactive drugs.
[108] Office for Human Research Protection in the Department of Health and Human Services. Guidance on Certificates of Confidentiality. Background. Feb 252003. [Accessed June 24, 2010]. http://www.hhs.gov/ohrp/humansubjects/guidance/certconf.htm.
[109] National Institutes of Health. Notice NOTOD-02-037. Mar 152002. [Accessed June 24, 2010]. http://grants1.nih.gov/grants/guide/notice-files/NOT-OD-02-037.html.
[110] Information about obtaining a certificate of confidentiality is available at the "CoC Kiosk" on the NIH Web site. [Accessed June 24, 2010]. Available at http://grants.nih.gov/grants/policy/coc/index.htm.
[111] National Institutes of Health, Office of Extramural Research. Certificates of Confidentiality: Background Information, Web posting. Feb 142006. [Accessed June 24, 2010]. http://grants.nih.gov/grants/policy/coc/background.htm.
[112] Information about certificates of confidentiality is available at the "CoC Kiosk" on the NIH Web site. [Accessed June 24, 2010]. Available at http://grants.nih.gov/grants/policy/coc/index.htm.
[113] 42 USCS 290dd-2 and 290ee-3; 42 CFR Part 2.
[114] 42 CFR 2.52(a).
[115] 42 CFR 2.52(a).
[116] Louisiana statute re protection of tobacco data from subpoena.

[117] See, for example, Wis. Stat. 146.38.
[118] See 45 CFR 164.512(i) and 46.116(d), respectively.
[119] 45 CFR 164.512(i)(2)(ii).
[120] 45 CFR 164.512(i)(1)(i).
[121] 45 CFR 164.512(i)(2).
[122] 45 CFR 164.512(i)(2)(iii) and (iv).
[123] 45 CFR 46.116(d).
[124] 21 CFR 50.20 and 50.23.
[125] 45 CFR 46.117(c)(1).
[126] 45 CFR 46.117(c)(2).
[127] 45 CFR 46.117(c).
[128] 45 CFR 164.528(a)(1).
[129] 45 CFR 164.528(b).
[130] 45 CFR 164.528(a)(1).
[131] 45 CFR 164.528(b)(3) and (4).
[132] 42 CFR 3.
[133] Kohn LT, Corrigan JM, Donaldson MS.Committee on Quality of Health Care in America, Institute of Medicine. To Err Is Human: Building a Safer Health System. Nov 1, 1999.
[134] See 73 Fed. Reg. 70,739.
[135] 42 C.F.R. § 3.20.
[136] 42 CFR 3.204.
[137] 42 CFR 3.206.
[138] 73 FR 70781 (November 21, 2008).
[139] 42 CFR 3.102.
[140] 42 U.S.C. 299b–22(i).45 C.F.R. § 164.501; 78 Fed. Reg. at 5592.
[141] Nass SJ, Levit LA, Gostin LO, editors. Committee on Health Research and the Privacy of Health Information. Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. National Academies Press; The HIPAA Privacy Rule; Institute of Medicine. http://www .nap.edu/catalog/12458.html.
[142] Beyond the HIPAA Privacy Rule, page 26.
[143] 45 CFR § 164.502(a)(3); 78 Fed. Reg. at 5660-61.
[144] HITECH Act §13404(a); 45 C.F.R. § 164.104(b); 78 Fed. Reg. at 5591.
[145] 74 F.R. 42740 (August 24, 2009); 45 C.F.R. § 164.402; 78 Fed. Reg. at 5641-44.
[146] 45 CFR 46.116(d)(4).
[147] The Center for International Blood and Marrow Transplant Research. [Accessed June 30, 2010]. http://www.cibmtr.org/index.html.
[148] 67 F.R. 53213, August 14, 2002.
[149] 67 F.R. 53213, August 14, 2002.
[150] Joyce C, Patry W, Leaffer M, et al. Copyright law. 3rd Edition. New York and San Francisco: Matthew Bender & Co., Inc; 1994. pp. 1–41. reprinted 1997. "The Landscape of Copyright."
[151] American Medical Association House of Delegates, Connecticut Delegation: Guiding Principles, Collection and Warehousing of Electronic Medical Record Information. Resolution #802. Sept 162005. [Accessed June 24, 2010]. http://www.ama-assn.org/meetings/public/interim05/802i05.pdfBailey S. Your data for sale? Boston Globe. Mar 242006. [Accessed June 24, 2010]. http://www.boston.com /business/healthcare/articles/2006/03/24/your_data_for_sale/
[152] American Recovery and Reimbursement Act section 13405(d)(2)(B).
[153] Washington University v. Catalona, Case No. 4:03CV1065SNL (E.D. Mo., filed Mar. 31, 2006). Washington University v. William J. Catalona, M.D., No. 06-2286 and No. 06-2301 (8th Cir. June 20, 2007).

[154] American College of Epidemiology. Policy Statement on Sharing Data from Epidemiologic Studies. May2002. [Accessed June 30, 2010]. Available at http://www.acepidemiology .org/policystmts/DataSharing.pdf.National Institutes of Health, U.S. Department of Health and Human Services. Final NIH Statement on Sharing Research Data, Notice NOT-OD-03-032. Feb 262003. [Accessed June 24, 2010]. Available at http://grants.nih.gov/grants/guide/notice-files/not-od-03-032.html.
[155] 78 FR 5566 at 5606 (January 25, 2013)
[156] 17 USC § 101.
[157] Feist Publications, Inc. v. Rural Telephone Service, Co., Inc., 499 U.S. 340, 345, 348 (1991).
[158] Id., 340 et seqHarris RK, Rosenfield SS Copyright Protection for Genetic Databases, 2005. Jurimetrics J. 45:225–250.(hereinafter Genetic Databases).